NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIFORNIA

THESIS

**SECURITY ISSUES
IN THE TELECOMMUNICATIONS PLAN
FOR CALS IMPLEMENTATION IN KOREA**

by

Kichan Bae

September, 1995

Thesis Advisor: Myung W. Suh
                                                   Rex Buddenberg

Approved for public release; distribution is unlimited.

19960221 052

REPORT DOCUMENTATION PAGE

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE September 1995	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE SECURITY ISSUES IN THE TELECOMMUNICATIONS PLAN FOR CALS IMPLEMENTATION IN KOREA		5. FUNDING NUMBERS	
6. AUTHOR(S) Bae, Kichan			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey CA 93943-5000		8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSORING/MONITORING AGENCY REPORT NUMBER	

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.	12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)*
Continuous Acquisition and Life-cycle Support (CALS) is an evolving strategy designed to take defense information from its current paper-intensive form to a totally electronic mode of operation by means of information integration and automation. To take full advantage of CALS, it is essential to accommodate distributed CALS computer networks, and to enable the interconnection of selected heterogeneous components in the networks. However, as CALS telecommunications deals with multi-level security data, it is critical to incorporate adequate security plans into the telecommunication plan. This thesis analyzes the requirements for a secure telecommunications plan that includes telecommunications standards and protocols, data exchange protocols, transmission media, and methods of network security necessary to implement CALS in the Korea defense environment. Literature reviews and expert interviews are used to support findings and conclusions. To accomplish a fully digitized CALS environment, the author concludes that proper data protection standards and methods must be provided and tested as part of the overall CALS telecommunications architecture. Enabling technology and a responsive management infrastructure must be in place to ensure successful implementation of CALS. The decision to select mechanisms should be made based on the comparison between security and integrity, in terms of efficiency, effectiveness, and availability.

14. SUBJECT TERMS Continuous Acquisition and Life-cycle Support (CALS), Electronic Commerce/Electronic Data Interchange (EC/EDI), and Network Security	15. NUMBER OF PAGES 146
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

SECURITY ISSUES IN THE TELECOMMUNICATIONS PLAN FOR CALS IMPLEMENTATION IN KOREA

Bae, Kichan
Captain, Republic of Korea Army
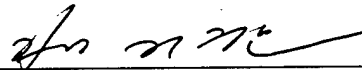B.A., Korea Military Academy, 1990

Submitted in partial fulfillment
of the requirements for the degree of

**MASTER OF SCIENCE IN
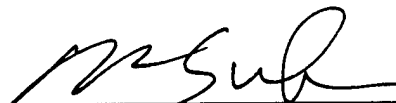INFORMATION TECHNOLOGY MANAGEMENT**

from the

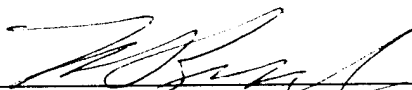**NAVAL POSTGRADUATE SCHOOL
September 1995**

Author: _____
Bae, Kichan

Approved by: _____
Myung W. Suh, Thesis Advisor

_____
Rex Buddenberg, Associate Advisor

_____
Reuben T. Harris, Chairman
Department of Systems Management

ABSTRACT

Continuous Acquisition and Life-cycle Support (CALS) is an evolving strategy designed to take defense information from its current paper-intensive form to a totally electronic mode of operation by means of information integration and automation. To take full advantage of CALS, it is essential to accommodate distributed CALS computer networks, and to enable the interconnection of selected heterogeneous components in the networks. However, as CALS telecommunications deals with multi-level security data, it is critical to incorporate adequate security plans into the telecommunication plan.

This thesis analyzes the requirements for a secure telecommunications plan that includes telecommunications standards and protocols, data exchange protocols, transmission media, and methods of network security necessary to implement CALS in the Korea defense environment. Literature reviews and expert interviews are used to support findings and conclusions.

To accomplish a fully digitized CALS environment, the author concludes that proper data protection standards and methods must be provided and tested as part of the overall CALS telecommunications architecture. Enabling technology and a responsive management infrastructure must be in place to ensure successful implementation of CALS. The decision to select mechanisms should be made based on the comparison between security and integrity, in terms of efficiency, effectiveness, and availability.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

ACL	Access Control List
ACM	Access Control Matrix
ADP	Automated Data Processing
AIS	Automated Information System
ANSI	American National Standards Institutes, Inc.
ASCII	American Standard for Information Interchange
ATM	Asynchronous Transfer Mode
CAD	Computer Aided Design
CALS	Continuous Acquisition and Life-Cycle Support
CAM	Computer Aided Manufacturing
CCITT (ITU-T)	Consultative Committee on International Telegraph and Telephone (renamed to International telecommunications Union-Telephone)
CDRL	Contract Data Requirement List
CE	Concurrent Engineering
CERT	Computer Emergency Response Team
CIM	Computer Integrated Manufacturing/Corporate Information Management
CITIS	Contractor Integrated Technical Information Service
CM	Configuration Management
CTN	CALS Test Network
DAC	Discretionary Access Control
DCN	Defense Logistics Agency Corporate Network
DCTN	Defense Commercial Telecommunications Network
DDN	Defense Data Network
DES	Data Encryption Standard
DISA	Defense Information Systems Agency
DISN	Defense Information System Network

DLA	U.S. Defense Logistics Agency
DoD	U.S. Department of Defense
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
DTD	Document Type Declaration
EC/EDI	Electronic Commerce/Electronic Data Interchange
EDCARS	Engineering Data Computer Retrieval System
EDIF	Electronic Design Interchange Format
EDIFACT	EDI for Finance, Administration, Commerce, and Transport
EDS	Electronic Display System
EFT	Electronic Funds Transfer
EI	Enterprise Integration
EIA	Electronic Industries Association
FDDI	Fiber Distributed Data Interface
FIPS	Federal Information Processing Standard
FIRP	Federal Internetworking Requirement Panel
FMECA	Failure Modes, Effects, and Criticality Analysis
FOSI	Formatting Output Specification Instance
FTS-2000	Federal Telecommunications System 2000
GDD/D	Global Data Dictionary and Directory
GFI	Government Furnished Information
GOSIP	Government Open Systems Interconnection Protocol
HTTP	HyperText Transfer Protocol
ICW	Interactive Courseware
IDEA	International Data Encryption Algorithm
IETF	Internet Engineering Task Force
IETM	Interactive Electronic Technical Manual
IGES	Initial Graphics Exchange Specifications

ILS	Integrated Logistics Support
IPC	Institute for Interconnecting and Packaging Electronic Circuits
IPNG	Internet Protocol Next Generation
IRDS	Information Resource Dictionary System
ISDN	Integrated Service Digital Network
ISG	Industry Steering Group
ISO	International Standards Organization
ISODE	ISO Development Environment
IWSDB	Integrated Weapon Systems Data Base
JCALS	Joint Computer-aided Acquisition and Logistics Support
JEDMICS	Joint Engineering Data Management Information and Control System
KDDN	Korean Defense Data Network
KII	Korean Information Infrastructure
LAN	Local Area Network
LSA	Logistic Support Analysis
LSAR	Logistic Support Analysis Record
MAC	Mandatory Access Control/Message Authentication Code
MAP	Manufacturing Automation Protocol
MHS	Message Handling Service
MISSI	Multilevel Information Systems Security Initiative
MND	Ministry of Defense of South Korea
NCSC	National Computer Security Center
NII	National Information Infrastructure
NIST	National Institute of Standard and Technology
NKN-G	New Korea Net-Government
NKN-P	New Korea Net-Public
NSA	National Security Agency

NSAD	Network Security Architecture and Design
NTCB	Network Trusted Computing Base
OSI	Open Systems Interconnection
PDES	Product Data Exchange using STEP
PDL	Page Description Language
PEM	Privacy Enhanced Mail
PGP	Pretty Good Privacy
PKCS	Public Key Cryptography Standard
PMRT	Program Management Responsibility Transfer
POSIT	Profiles for Open Systems Internetworking Technologies
PSSC	Preliminary System Security Concept
RDA	Remote Database Access
RFQ	Request For Quote
SGML	Standard Generalization Markup Language
SHS	Secure Hash Standard
SHTTP	Secure HyperText Transfer Protocol
SMTP	Simple Mail Transfer Protocol
SONET	Synchronous Optical Network
SOW	Statement of Work
SQL	Standard Query Language
SSE	System Security Engineering
SSL	Secure Sockets Layer
SSMP	System Security Management Plan
STEP	Standard for the Exchange of Product Model Data
TCB	Trusted Computing Base
TCP/IP	Transmission Control Protocol and Internet Protocol
TCSEC	Trusted Computer System Evaluation Criteria
TDP	Technical Data Package

TGG	Trusted Guard Gateway
TNI	Trusted Network Interpretation
TNIEG	Trusted Network Interpretation Environment Guideline
TOP	Technical Office Protocol
TRM	Technical Reference Model
UCC	Uniform Commercial Code
VHDL	VHSIC Hardware Description Language
VHSIC	Very High Speed Integrated Circuit
WBS	Work Breakdown Structure

I. INTRODUCTION

A. OVERVIEW

The continuous growth of computer and information technologies is rapidly changing the way of doing business. Industries face an increased necessity to integrate and network for better quality and lower cost products and services or, in other words, for "doing more with less." Continuous Acquisition and Life-Cycle Support (CALS) promotes an environment where business processes for the design, development, manufacturing, distribution, and servicing of products are integrated and streamlined, based on a common digital database.

CALS was begun primarily as a strategy to improve the productivity and quality of weapon systems information at lower life-cycle costs by facilitating the integration of digital technical information for weapon system acquisition, design, manufacture, and support. Today, CALS has become recognized as a leading-edge prototype for the "virtual enterprise" in the twenty first century [Ref. 1].

In order to create an open systems environment, the CALS implementation strategy focuses on distributed databases, connected by local area and wide area networks that will provide the U.S. Department of Defense (DoD) and industry with direct access to information they need. While this evolutionary goal of modernizing information exchange will reduce the costs of data handling, and bring more timely and accurate data to users, protecting CALS data and its system components make the achievement of this system a challenging goal. Thus, appropriate protection of all the CALS data and components should be considered a vital part of CALS implementation strategy for the confidentiality and integrity of CALS data.

In the Korean defense environment, a reduced defense budget and the burden of paper-intensive data flows require a new way of dealing with information to acquire weapon systems and support its life-cycle maintenance at lower costs with better quality.

1

Also, as emerging information technologies (e.g., Concurrent Engineering (CE) and Electronic Commerce/Electronic Data Interchange (EC/EDI)) are becoming important parts of CALS, the effort to adopt CALS strategy has not only brought about the cooperation of Ministry of Defense (MND) and defense industry in Korea, but also affected competitive industries who want to pursue enterprise integration and industrial networking at a rapidly increasing pace.

Although CALS envisions highly profitable goals (e.g., reduced cost, integrated timely information, a paperless work place), those who want to launch this nation-wide project with little prior experience should carefully consider the current obstacles challenging the CALS implementation objectives.

B. OBJECTIVES

When an integrated data environment among various organizations -- including governmental and industrial organizations -- is realized via an electronic ally linking the dissimilar databases of these organizations, the concern for individual and organizational confidentiality is also growing. Therefore, the success of CALS is contingent upon finding a reasonable balance between security and effective data sharing [Ref. 2].

As a part of the effort to find a balance between data integrity and security, this thesis will investigate the methods to secure CALS data via telecommunications architecture for the CALS implementation. The primary objective of this research is to define the secure telecommunications plan for the implementation of CALS in the Korean defense environment. To achieve the primary objective, this research assesses: (1) required components of CALS telecommunications including standards, data transmission requirement, and network infrastructure, (2) necessary protection methods for the telecommunication channel and data itself, and (3) appropriate security management for the secure telecommunications architecture.

C. SCOPE AND ORGANIZATION

This thesis begins by briefly reviewing the CALS initiative and its strategies. To present secure telecommunications architecture required for the CALS implementation, the data transmitted via CALS network, the components of CALS network, and the protection methods for CALS data will be analyzed. Although CALS security includes physical security in a trusted computer system, multi-level secure database management systems, and many other issues, this thesis will focus primarily on network issues related to CALS telecommunications plan.

This thesis is organized in six chapters. Chapter II, Continuous Acquisition and Life-Cycle Support (CALS), presents the background of CALS and its critical components. Chapter III, CALS Telecommunications Plan, analyzes requirements for the CALS data transmission. Chapter IV, Network Security and Related Issues, presents current protection methodologies related to the CALS network security and data protection. Chapter V, Security Management of CALS Telecommunications, overviews relative security policies and standards, and then presents a secure telecommunications architecture for the CALS implementation in Korea. Finally, Chapter VI, Conclusion, presents conclusions drawn from this research and discusses further research requirements.

4

II. CONTINUOUS ACQUISITION AND LIFE-CYCLE SUPPORT (CALS)

CALS is defined as a Department of Defense (DoD) and industry strategy to enable more effective generation, exchange, management, and use of digital information that supports the life cycle of a product through the use of national and international standards, business process changes, and advanced technology applications. [Ref. 3] In this Chapter, the history, strategy, and standards and specifications for CALS are presented briefly. Next, the key components to enable the goals of CALS are described.

A. BACKGROUND

1. History of CALS

In September 1985, CALS (which then stood for "Computer-Aided Logistics Support") was officially initiated by a memorandum from the U.S. Deputy Secretary of Defense to implement the recommendations of a Joint Industry/DoD Task Force in an effort to standardize digital encoding of technical information [Ref. 4]. At that time, several emerging technologies stimulated new thinking about managing and publishing logistics technical information. Those new technologies enabled a transition from paper-based documents to ones that are created, delivered, used, and maintained in digital form. CALS reduces costs by enabling users to buy information that is more accurate, current, timely, and entered once and used many times.

The opportunities offered by CALS technologies spread quickly to encompass weapon systems acquisition information. By 1988, CALS expanded to include acquisition and stood for "Computer-aided Acquisition and Logistics Support." It could be said that CALS was officially launched by a memorandum from Deputy Secretary of Defense dated 5 August 1988 [Ref. 5: p. 6]. At the end of 1989, CALS added the discipline of concurrent engineering (CE) to incorporate the design process with weapon system production and logistics support processes.

At the same time, other digital information technologies, such as electronic commerce/electronic data interchange (EC/EDI), enabled the computer-to-computer exchange of business information. EDI dramatically reduces the costs of business transactions, largely by eliminating re-keying of data. EDI also provides the means to integrate business functions, enable process improvements, and establish extended enterprises.

As CALS has grown, so has its acceptance and use by the international community. Government and commercial users have organized to develop CALS further in Europe and the Pacific Rim, as well as in the United States and Canada. In 1993, the definition of the acronym was changed once again to "Continuous Acquisition and Life-cycle Support." This most recent change was meant to reflect the fact that CALS is a strategy for information and process improvement, and that both are continuous. This latest focus recognizes CALS as a facilitator for world-wide process improvement and enterprise integration. [Ref. 6, p. 17]

2. CALS Development Strategy

MIL-HDBK-59B clearly states the military aspects of the primary goal of the CALS as "to migrate from manual, paper-intensive defense system operations to integrated, highly automated acquisition and support process" [Ref. 7: p. 4]. A target of these automated and integrated processes will be the Integrated Weapon Systems Data Base (IWSDB). Figure 1 shows how the IWSDB is accomplished throughout the life of a defense system.

First, to support uniform integrated and interrelated digital-based functional processes among all services and the Defense Logistics Agency (DLA), the infrastructure -- including computer hardware, software, and communication network capabilities -- is required to be modernized under a standards-driven, open-system architecture, which gives interoperability within industry and the DoD defense system.

6

Second, based on the modernized infrastructure, business process re-engineering is required in design, manufacturing, and life-cycle support of a defense system. Examples of the process improvements are direct coupling of design processes and integrated databases, elimination of duplicative, manual, error-prone processes, use of digital data, use of electronic data interchange, and development of integrated design and manufacturing capabilities with industry teaming arrangements.

Third, migration from paper-based data to digital data will be accomplished by the use of common interfaces and neutral file formats, as defined in the standards and specifications that support information sharing and exchange across dissimilar computer systems.

Finally, by implementing the previous three steps, logical data structure that can control and coordinate all technical information used to support a weapon system throughout its life-cycle will be accomplished by the IWSDB. DoD anticipates an effective shared environment where government and industry participate via this database concept.
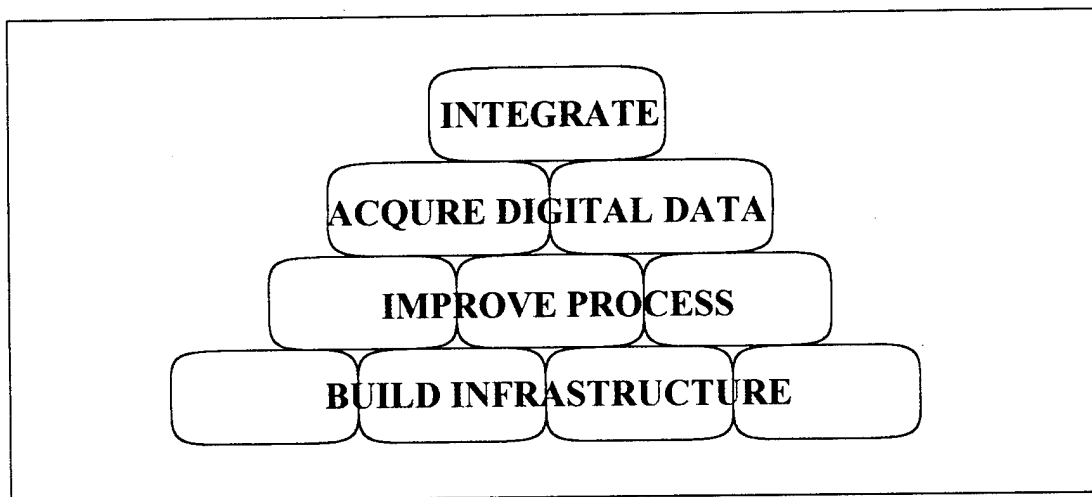
Figure 1. Foundation for Creation, Management, and Use of Digital Data [Ref. 7]

Another definition of CALS is "a global strategy to further enterprise integration through the streamlining of business processes and the application of standards and technologies for the development, management, exchange, and use of business and technical information" [Ref. 6: p. 18]. This statement shows the industrial aspects of CALS as a strategy to find the most efficient way of doing business through sharing of standardized information by removing information barriers and redundant or unnecessary business processes via international coordination and cooperation. This tendency reflects the facts that CALS' domain is not necessarily limited in the relationship between DoD and the defense industry, and CALS is accepted by industry as a survival strategy in the highly competitive international business environment.
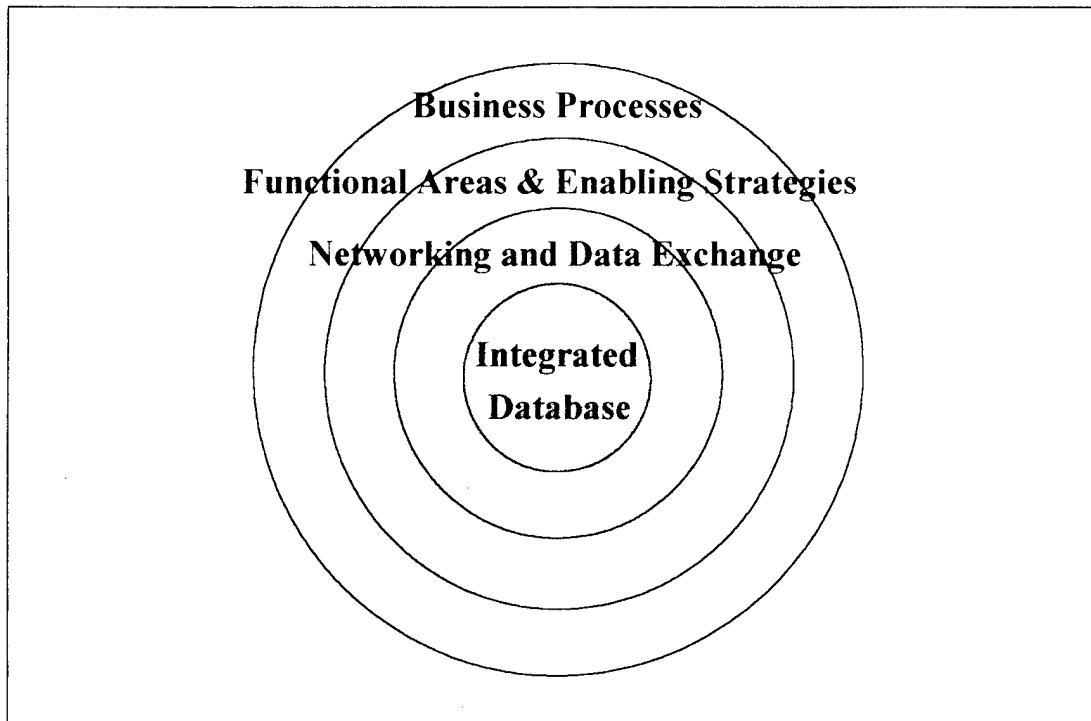
Figure 2. The CALS Environment [Ref. 6: p.28]

To implement an Integrated Data Base (IDB), CALS Industry Steering Group presented a similar approach to the government's [Ref. 6]. In Figure 2, The outermost

ring indicates the necessity of business re-engineering from old business processes, which were established with paper formats and no longer apply in an electronic information environment. It is a client-centered approach, in which a workflow analysis is used to streamline or redesign the business processes and optimize organizational efficiency. The second outermost ring indicates that a redesigned organization's functional processes will be closely tied together to operate more efficiently by the use of enabling strategies, including Concurrent Engineering (CE), Computer Integrated Manufacturing (CIM), and Integrated Logistics Support (ILS). For the Networking and Data Exchange, which provides the role of electronic information bridge, the use of Electronic Commerce (EC)[1] is suggested. Finally, to make an IDB work, establishment of Contractor Integrated Technical Information Service (CITIS), development of global data dictionary, and use of Configuration Management (CM) are also suggested. [Ref. 6]

3. CALS Standards and Specifications

Standards are fundamental for CALS success. DoD CALS Evaluation and Integration Office is adopting and developing data and information standards and specifications to provide the common interface and neutral file formats necessary for the effective interchange and efficient use of digital technical data. DoD CALS policy on the CALS standards is to use existing and emerging national and international standards wherever possible to achieve this objective.

Initially, CALS is focusing on standards for the electronic interchange of digital technical information among dissimilar computer systems. These initial CALS standards are intended to enable the digital delivery of engineering drawings, illustrations, technical manuals, and engineering data [Ref. 8: p. 12-5].

---

[1]   In this context, EC may include EDI, E-mail, electronic bulletin boards, electronic funds transfer (EFT), and other similar technologies.

Table 1. CALS Standards and Specifications [Ref. 8: p. a-16]

DoD	Industry	Applications
MIL-HDBK-59		Provide guidance on the technology, standards, and procurement process as related to the transition from a paper-intensive activity to one operating with digital information.
MIL-STD-1840		The primary defense standardization document for the selected CALS standards. Identifies, by application, which industry standard and corresponding DoD standardization documentation to use. It also provides standard "enveloping" procedures for transferring standard data forms.
MIL-D-28000	IGES	Initial Graphics Exchange Specifications (IGES) - A neutral file format for the representation and transfer of product definition data among CAD/CAM systems and application programs.
MIL-M-28001	SGML	Standard Generalization Markup Language (SGML) - Markup requirements, tagging, and generic style specifications for page-oriented document text.
MIL-R-28002	CCITT GROUP 4	The efficient compression of scanned raster images. Uses the code from the group 4 facsimile recommendation of the International Telegraph and Telephone Consultative Committee (CCITT). A "tiled" form is described by using the architecture nomenclature of International Standard, ISO 8613.
MIL-D-28003	CGM	Computer Graphics Metafile (CGM) - A neutral format for the description, storage, and communication of graphical information.
FIPS 161	EC/EDI	Electronic Commerce/Electronic Data Interchange (EC/EDI) - The electronic interchange of business information between trading partners. Uses standard formats currently defined by ANSI x12 in the U.S., EDIFACT in Europe, and AECMA 2000 for NATO.
ISO 10303	STEP	Standard for the Exchange of Product Model Data (STEP) - A computer interpretable data representation format being developed to include all product throughout its life cycle. Product Data Exchange using STEP (PDES) is the U.S. standards activity supporting STEP.
MIL-STD-974	CITIS	Contractor Integrated Technical Information Service (CITIS) - Contractor provided service for electronic access and/or delivery of contractually committed business and technical information on a need to know basis.
MIL-M-87268	IETM	Prescribes the requirements governing the creation of Interactive Electronic Technical Manual (IETM) and the development of IETM presentation software applicable to a computer-controlled Electronic Display System (EDS).
MIL-D-87269	IETM	Prescribes the interchange format for delivery of an IETM database to the Government.
MIL-Q-87270	IETM	Prescribes the requirements for an IETM Contractor's Quality Assurance (QA) program.
MIL-HDBK-SGML (draft)	SGML	Provides guidance in the application of MIL-M-28001, which is based on ISO 8879, Standard Generalized Markup Language. Data prepared in accordance with these guidelines will facilitate the automated storage, retrieval, interchange, and processing of technical documents from varied data sources.

As CALS standards and specifications reflect the current trends and future directions for the fully integrated CALS digital environment, further standards will focus on complete product definition data, product models, and the need to access and manage data within distributed database environments to meet long term CALS capability (shown in the previous sub-section). Table 1 shows a list of DoD standards and their descriptions commonly used by industry as a reference for the CALS implementation.

MIL-HDBK-59B presents two additional types of standards: other digital data interchange standards, and product, process, data integration standards. Certain industry standards for digital data interchange provide the opportunity for the acquisition of intelligent data necessary to support specific applications for defense systems. Table 2 shows these standards and their applications. As these standards are not yet officially endorsed as CALS standards, they will be used by mutual consent between government and contractor.

Table 2. Digital Data Interchange Standards

Standards	Applications
VHDL	Very High Speed Integrated Circuit (VHSIC) Hardware Description Language (VHDL) - ANSI/IEEE 1076. A formal notation intended for use in all phases of the creation of electronic systems. Supports the development, verification, synthesis, and testing of hardware designs, the communication of hardware design data, and the maintenance, modification, and procurement of hardware.
EDIF	Electronic Design Interchange Format (EDIF) - ANSI/EIA 548-1988. Define the exchange of electronics product data between diverse CAD hardware and software. Designed to address all concerns shared by the electronic design community, including simulation models, schematics, and integrated circuit layouts.
IPC-D-350	Printed Board Description In Digital Form. Specify 80-character, fixed-length record formats used to describe printed-circuit board products with detail sufficient for tooling, manufacturing, and testing requirements. Transmit information in digital form between design and manufacturing facilities.

In addition, product, process, and data integration standards reflect the present effort toward CALS implementation in the acquisition process on the integrated design,

development and manufacturing environment. Table 3 shows the military standards and their applications.

Table 3. Product, Process, and Data Integration Standards

Standards	Applications
MIL-STD-499	Engineering Management. Assists in defining, performing, managing, and evaluating the systems engineering process efforts in defense systems acquisitions and technology developments. Implements technical essence of Concurrent Engineering and supports integrated product and process development.
MIL-STD-881	Work Breakdown Structure (WBS) for Defense Material Items. Establishes criteria governing the preparation and employment of WBS for use during the acquisition of designated defense materiel items.
MIL-STD-973	Configuration Management (CM). Sets forth CM practices that are to be tailored to specific programs and implemented by the contract SOW language. Applies technical and administrative direction over the life-cycle of configuration items, and describes in technical documentation the functional and physical characteristics of existing or planned hardware and software to meet product development and mission needs.
MIL-STD-1388-1	Logistic Support Analysis. Provides general requirements and task descriptions governing performance of logistic support analysis during the life-cycle of systems and equipment.
MIL-STD-1388-2	Logistic Support Analysis Report. Prescribes the data element definitions, data field lengths, and formats for LSAR data. Allows for delivery of LSAR data in manual or automated mode and on-line access to LSAR data as specified by the requiring authority.

Since the initiation of CALS in 1985, continuous efforts to revise CALS standards have taken place in the guideline standards, neutral file format standards, or specific application related standards to match the rapidly advancing information technology and to reflect the result of tests being done on the current CALS standards. As CALS evolves toward integrated data bases, whether it is weapon system data base or industrial technical data base, it is wise to keep up with new drafts and amendments as they are issued. One example of these revising efforts was shown in the Bergmann memo, which allows the use of revised interface standards and performance specification without waivers [Ref. 9]. Another example is the revision of MIL-STD-1840, which serves as a central standard for

the CALS environment. The next version of this standard is expected in late 1995 [Ref. 8: p. 12-9].

For its decade-long evolving history, CALS has developed new standards or adopted other commercial standards to keep up with the advance of information technology and industry trends. However, as a result of this history, there are some functional redundancies among these standards. It gives a selection problem to those who recently try to adopt CALS. A CALS-compliant standard does not mean that it is the most applicable standard for the particular requirement of application. For this reason, Knox et al. presented a way to categorize CALS standards [Ref. 10: p. 67 - 71]. This categorization is summarized in Table 4.

Table 4. Categorized Application Specific CALS Standards

Category	function	example of CALS standard
Data transportation	Moving data form one location to another. Concerned mainly with error-free transfer of data. Content independent. (enveloping)	MIL-STD-1840A TCP/IP (RFC 791/793) GOSIP (FIPS 146-1)
Data management	Storing, retrieving, and updating data. Cover language, data dictionary, distributed data. Content independent.	SQL (FIPS 127) IRDS (FIPS 156) RDA (draft ISO standard)
Data representation	Formatting data in a standard manner. Interpretation of data Content dependent.	EDI (FIPS 161) IGES (MIL-D-28000) SGML (MIL-STD-28001) Raster (MIL-STD-28002) CGM (MIL-STD-28003) PDES/STEP (ISO 10303) LSA/R (MIL-STD-1388)

Data representation standards reflect the intensive effort of CALS to achieve automation and integration of data existing in the dissimilar formats. These are presented in Figure 3 by the relationship between information richness[2] and requisite human

---

[2] Data is "information rich" in inverse proportion to the amount of human processing or intervention that is required to make the data useful. To require no human processing to generate data, there should be more products and actions. [Ref. 10: p.67]

intervention. Thus, the use of different data representation standards depends on the different stages of product's life-cycle. For example, the more stages the product has, the richer the standard description of the product must be [Ref. 10].
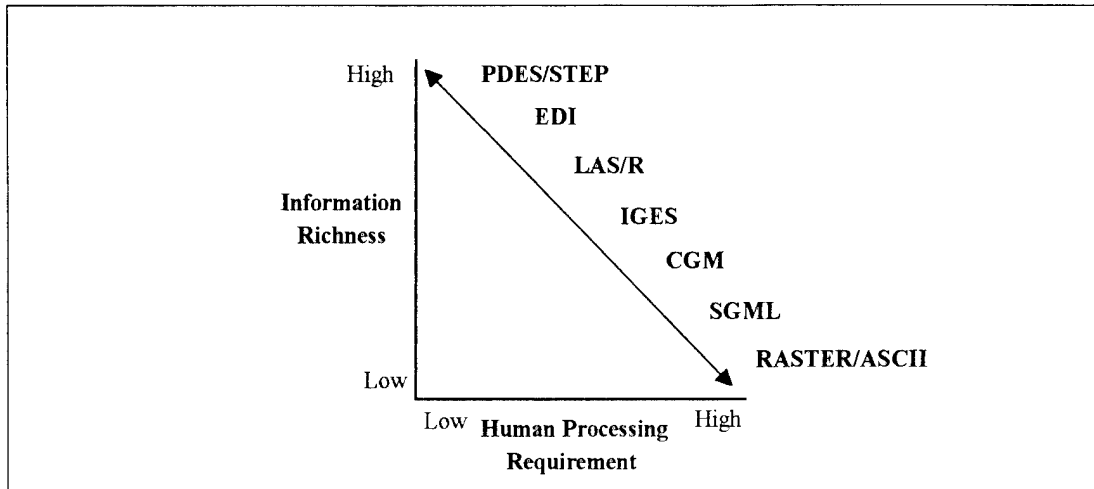
**Figure 3. Information Richness, Human Processing Requirements, and Standards
[Ref. 10: p. 69]**

B. CALS ENABLER

1. Government/Industry Roles

To achieve integrated data environment, collaboration for planning, managing, and implementing CALS between DoD and industry is definitely required. Figure 4 shows the various organizations, their role, and the relationships. The role of the DoD CALS Steering Group is to formulate CALS policy, to provide executive direction, and to implement the CALS program within DoD, whereas the role of the Industry Steering Group is to provide the focal point for CALS planning, technology and implementation concerns within industry. These two groups have been working together, holding joint meetings, and jointly acting as the corporate board of directors [Ref. 5: p. 11].

14
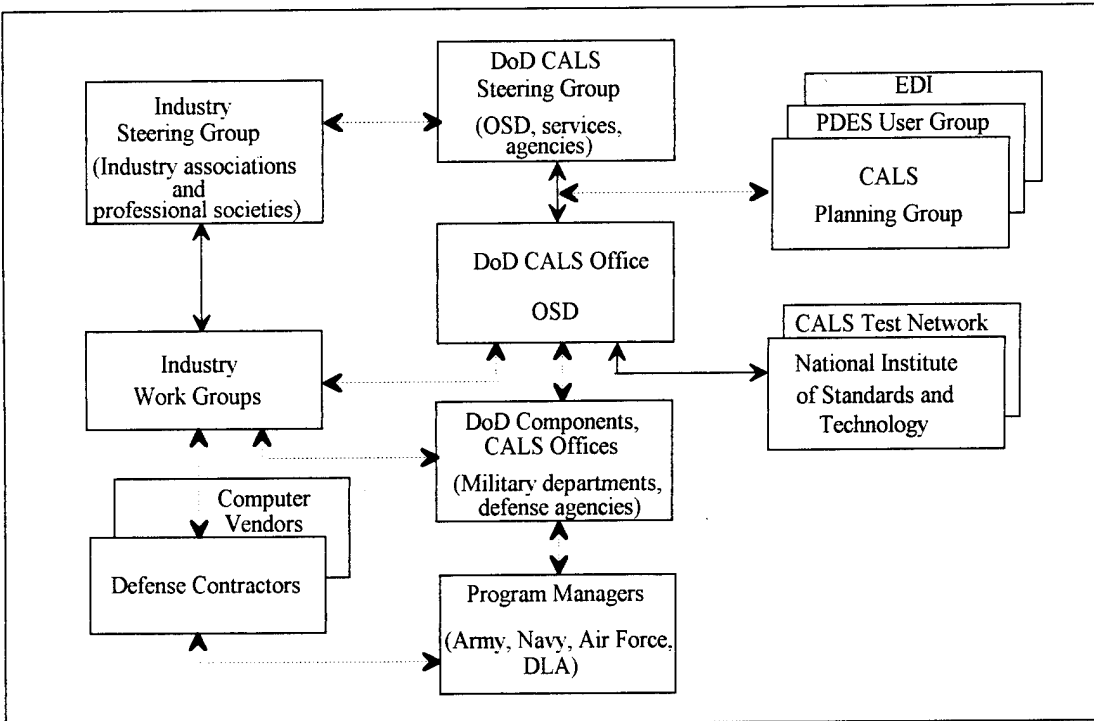
Figure 4. The CALS Management Organization [Ref. 11]

Charted DoD CALS organizations and other related government organizations take various roles to implement CALS strategy into their own domain. However, it is the responsibility of the DoD CALS Steering Group to provide coordination and guidance to ensure that there is no unnecessary duplication among the CALS acquisitions made by the DoD components. As mentioned in the previous section, to achieve IWSDB, the efforts of DoD should be concentrated on the modernization of its own infrastructure, coordination of DoD process improvement among all services and DLA, acquisition of digital data using commercial CALS technology, and continuous monitoring of the current implementation of the CALS vision.

The Industry Steering Group (ISG) has several committees to cover many of the areas crucial to the success of CALS: concurrent engineering, information management, education and training, logistic process, small businesses, acquisition, and international considerations. These committees highlight areas in which further work has to be done,

such as information management, and they address topics of concern, such as the effect of CALS on small businesses [Ref. 5: p. 16]. Ongoing development of information technology toward integrated data environment and wide adoption of CALS as a strategy to improve business processes will make the role of ISG much broader.

2. CALS Infrastructure

Generally speaking, an infrastructure is a set of resources used by more than one information system. More specifically, the CALS infrastructure is the underlying foundation or basic framework required for the creation, exchange, management, and use of digital data in a CALS environment [Ref. 7: p. 55]. This underlying foundation required in a CALS environment includes computer hardware, software, and communication network capabilities. To achieve IWSDB, fundamental changes are required to modernize these components in the way DoD receives and uses technical data. To be able to receive, transmit, and utilize digital data in the management of weapon systems and related support activities, the DoD addressed two means of infrastructure modernization as:

- Development of a joint service system that embodies the target system design and functional attributes and provides a fully encompassing infrastructure for evolving complementary system; and

- Modification of existing and near-term planned systems for evolution towards CALS requirements and the target system concept.

The efforts of DoD to modernize infrastructure toward a cost-effective CALS solution for acquiring and managing information by means of joint service system development are well reflected in Joint Computer-aided Acquisition and Logistics Support (JCALS) and Joint Engineering Data Management Information and Control System (JEDMICS).

JCALS is an information management system that is evolving to support uniform logistic, acquisition, engineering, manufacturing, configuration management, material management, and other life-cycle functional processes. The JCALS concept originated from the US Army's Technical Information Management System (TIMS), and then became the Army CALS (ACALS) program in March 1987. In January 1991, the Army was directed to transit ACALS to JCALS to include joint requirements and to make it a joint program.

Actually, JCALS was designed according to CALS requirements and Corporate Information Management (CIM) Technical Reference Model (TRM) architecture. JCALS uses multi-weapon system IWSDBs and Global Data Dictionary/Directory (GDD/D) Services that are connected by a wide area computer network. The interface for users provides an environment to access all of JCALS's functionality transparently with a need-to-know and proper access privileges. To make JCALS more flexible and scaleable, and to avoid further major re-engineering, use of open system architecture standards, modular hardware, and data-driven modular software design is required. [Ref. 7: p. 34]

JEDMICS is a CALS-compliant repository for the storage of engineering drawings and related technical data. It originated from the Engineering Data Management Information and Control System (EDMICS) initiated by Navy. The EDMICS program was validated as a program meeting the CALS initiative strategies and objectives in 1991, and selected as a tri-service program later that year. In 1993, EDMICS was chartered as a joint program by DoD, and renamed JEDMICS. JEDMICS consists of six subsystems[3] that permit users on-line access to engineering drawings and related technical data stored in CALS data formats. These subsystems follow a standard open system design in a client-server architecture. The subsystems are scaleable and compatible with existing applications and information systems at a particular JEDMICS site. [Ref. 12: p. 27]

---

[3] These subsystems are input, data integrity, index, storage, output, and remote output subsystem.

The modification of existing and near-term planned systems, suggested as a means to modernize DoD information infrastructure, is not an easy task. Prior to applying CALS to these systems, the characteristics of the program (i.e., program phase, type, size, and duration), the expected data conversion impact (i.e., data size, data sensitivity, required operating systems, and existing DoD infrastructure capabilities) and the result of cost/benefit analysis should be carefully considered. After these consideration, approaches on this modification will be (1) contract modification or (2) incentive programs that encourage the contractor and their subcontractors to undertake modernization projects [Ref. 7: p. 29-32].

To reduce further bridging cost required to achieve IWSDB, the two approaches for infrastructure modernization should be closely coordinated by the use of open system standards and CALS data standards. Also, to achieve interoperability with industry who are providing the major input to the defense system, continuous evolution of common and consistent applications of Contractor Integrated Technical Information Service (CITIS) is required.

3. Concurrent Engineering (CE)

Concurrent Engineering (CE) is a systematic approach to the integrated, concurrent design of products and their related processes, including manufacturing and support. This approach is intended to cause the developers, form the outset, to consider all elements of the product life-cycle from conception through disposal, including quality, cost, schedule, and user requirements [Ref. 7: p.54]. CE simultaneously defines the product, its manufacturing processes, and all other required life-cycle processes, such as logistic support. It is not the arbitrary elimination of a phase of the existing, sequential, feed-forward engineering process, but rather the co-design of all downstream processes toward a more all-encompassing, cost-effective optimum. [Ref. 13: p. 55]

This approach came from the recognition that conventional product development practices (i.e., sequential isolated design, and repeated iteration procedure to correct

18

design flaws) became progressively less efficient as product complexity and market demands increase. By considering all aspects of a product's life cycle simultaneously and cross functionally, CE gives significant reductions in product development cycles, a wide range of cost savings, and substantial improvements in product quality. As the integration of Reliability and Maintainability (R&M) with CAD/CAE is a high-leverage, high-payoff CALS target area and CE can support this integration, currently CALS/CE environment[4] is espoused in the CALS policy.

However, to achieve the benefits of CE, development of appropriate tools for design, manufacturing, and quality assurance, networking capabilities for the proper integration among all participants with adequate access control and, most importantly, cultural changes to break down various barriers among engineer, manufacturer, and end user should be precede this environment.

4. Electronic Commerce/Electronic Data Interchange (EC/EDI)

Electronic Commerce (EC) has been defined as the conduct of business transactions, supporting functions such as administration, finance, logistics, procurement, and transportation, between the government and private industry, using an integrated automated information environment. Electronic Data Interchange (EDI) is one application of EC, defined as the electronic transmission of business information between two or more computers, across different computer platforms.

As EC/EDI can handle on-line, timely exchange of digitized information required for routine business, the use of EC/EDI provides many benefits to both information provider and user, more specifically to suppliers and government. Thus, the goal of EC/EDI is to mold the vast network of small businesses, government agencies, large corporations, and independent contractors into a single community with the ability to communicate with one another seamlessly across any computer platform.

---

[4] The DoD stated that "Product, process, and data integration enhance a design, development, manufacturing, and support environment that demonstrates functionally integrated government/industry teams working with shared data." [Ref. 7: p. 28]

To achieve this goal within DoD, a memorandum from the Deputy Secretary of Defense, dated May 1988, directed the maximum use of EDI and EC throughout DoD, a common approach to EC throughout DoD, and a single face to industry from all of DoD. The Defense Management Review Directive (DMRD) 941 EC/EDI, Implementation in the Procurement Process, dated November 1990, directed a very aggressive implementation schedule: 80% or more of their small-purchase contracts by the end of FY94 [Ref. 14: p.62]. According to the Federal Acquisition Streamlining Act of 1994 on September 1994, signed by President Clinton, government-wide implementation of electronic commerce for appropriate Federal purchases to the maximum extent possible will be completed by January 1997 [Ref. 15: p. 7].

Although EC/EDI was not initiated by CALS, telecommunication networks capabilities give an excellent opportunity to exchange and establish common practices for business type data delivery (i.e., procurement processes) without paper flows. For the past ten years, industry has had the ability to transmit this digitized information through the American National Standards Institute (ANSI) X12 standards for various transaction sets, such as an 840 Request for Quote (RFQ) or an 850 Purchase Order (PO). However, the transaction set for transferring digitized technical information wasn't developed and accepted as a standard until October 1990. With the approval of the ANSI X12 841 transaction set, which supports CALS-compliant technical and engineering data, and the issuance of FIPS 161 effective September 1991, contractors are able to incorporate technical data into RFQ in a CALS format in accordance with MIL-STD-1840 [Ref. 14: p. 62]. The latest revision of CALS Implementation Guide stated the use of EDI as "FIPS PUB 161 summarizes the adoption of the families of interrelated software standards known as ASC X12 and Electronic Data Interchange for Administration, Commerce, and Transport (EDIFACT) for electronic transmission of such data. The acquisition manager should consider taking advantage of this opportunity for program administration process improvements" [Ref. 7: p. 17].

5. Product Data Exchange Using STEP (PDES)

The Standard for the Exchange of Product Model Data (STEP) is the familiar name for the international standard ISO 10303 Industrial Automation Systems and Integration Product Data Representation and Exchange. It is the international standards effort to develop a neutral mechanism capable of completely representing product data throughout the life-cycle of a product. The completeness of this representation makes it suitable, not only for neutral file exchange, but also as a basis for implementing and sharing databases and archiving.

Though the official CALS specification for the CAD/CAE is IGES represented as MIL-D-28000, it has some drawbacks. First of all, IGES is not sufficient to cover all types of product data. This requires further revising efforts to develop subsets. Second, compared to CGM or STEP, the size of IGES data is relatively big, thus it is hard to deliver IGES file over current networks. A further drawback is that IGES addresses the exchange of product data only at the time of design work, not throughout the life cycle of the product [Ref. 5: p. 77]. STEP has potential capability to solve all of these drawbacks by providing product definitions covering the entire life-cycle, and supporting shared database environment. This is the reason why STEP is emphasized as a key element in the longer term CALS strategy for improving the productivity and quality of product design, manufacturing, and support.

Product Data Exchange using STEP (PDES) is the U.S. effort to promote STEP. It ensures that U.S. industry requirements are incorporated into STEP, and provides methodologies for the implementation of STEP standards. The intent of this activity is to support the cooperative effort to produce a single international standard. So, when standard is represented, the term STEP is more preferable.

STEP is a collection of standards, all covered under ISO 10303. They are divided into categories based on their function within the standards. The most important two categories are Generic Resources and Application Protocols (APs). The basic strategy of the STEP community is to create a set of APs that convert end-user requirements into

21

specifications that can be used to test conformance of vendor-implemented application software to the standard. The APs define the scope, the information to be exchanged, the means of testing, and a user's guide for implementing the application [Ref. 16: p. 80]. Generic Resources are used to develop the emerging APs by providing a generic set of basic product information entities such as tolerance, geometry, shape, material, drafting, and kinematics.

STEP is still immature, although there are numerous STEP pilot projects progressing through various stages of completion. At the CALS Expo '94, Long Beach, only twelve parts were initially released as international standards. However, it is anticipated that STEP will be an important contributor to IWSDB via Contract Integrated Technical Information Service (CITIS). This is one reason why Smith suggested early use of STEP in CALS to ease the migration from IGES to STEP [Ref. 5: p.80].

6. Integrated Weapon System Database (IWSDB)

Integrated Weapon System Database (IWSDB) is the final target of the DoD CALS strategy to migrate from manual, paper-intensive defense system operations to integrated, highly automated acquisition and support processes. The concept of IWSDB is the construction of a single, logical database which contains all technical information used to support a weapon system throughout its life-cycle. The DoD states that this database concept will provide the basis for government and industry to participate in an effective shared environment [Ref. 7: p. 5]. Figure 5 shows the concept of the IWSDB.

IWSDB is a multi-weapon systems repository that services all the functions related to product design, engineering analysis manufacture, and support. To match the concept of store-once-use-many-times, there will be vertical access to data bases within a single weapon systems, and horizontal access to data bases across different weapon systems [Ref. 5: p. 52].
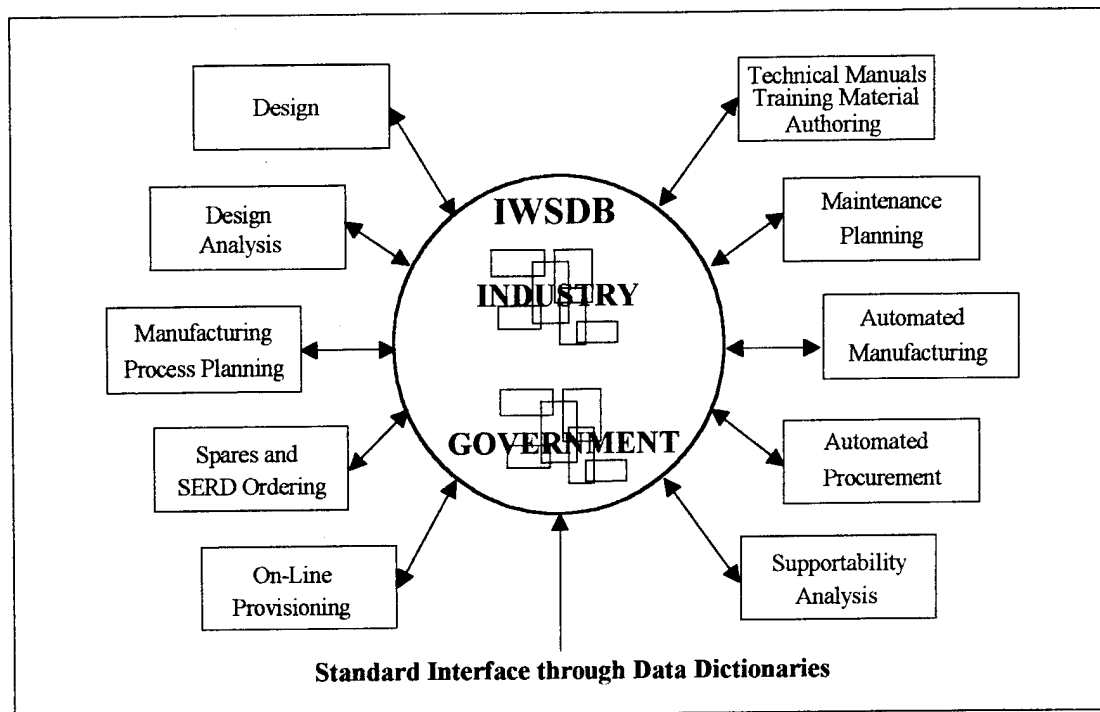
Figure 5. IWSDB [Ref. 5: p. 52]

In order to ensure data integrity and reduce data redundancy, the IWSDB will be supported by a data dictionary and data directory upon logically collected distributed data bases. The Global Data Dictionary and Directory (GDD/D) database is one approach to accomplish this goal. The GDD/D database will serve as a repository of data management policy and data integrity requirements for data stored in IWSDB [Ref. 7: p. 35]. In the JCALS system, the services required to access and manage the distributed data of the IWSDB will be provided by the Global Data Management System (GDMS).

The technology for interfacing between information providers and users continues to evolve. The Contractor Integrated Technical Information Service (CITIS), which is a contractor-developed service which provides electronic access to or delivery of contractually required CDRL to user, is a current DoD guidance for the bi-directional interface between government and industry. Also, the government encourages industry to use CITIS for a high degree of information integration across the enterprise and business partners. Although CITIS provides options for the on-line access and delivery of digital

23

data, current telecommunications capacity and relatively large size of engineering drawings make it inefficient. However, use of the mature STEP will support the IWSDB not only by reducing actual file size but also providing product definitions throughout the life-cycle of weapon system.

Smith stated that configuration management of technical information is another key issue [Ref. 5: p. 55]. The government could choose to have interactive access to the different types of data (i.e., working, released, submitted, and approved) in the CITIS rather than accept it as a deliverable. There are many aspects to configuration management; for example, the contractor will have to maintain in his status accounting system a complete change history for data files. As one of the product, process, data integration standards, MIL-HDBK-59B presents MIL-STD-973 Configuration Management (CM).

When integrity of information is increasing, the fear for the secrecy and privacy of information is increasing, too. One of the most challenging goals is to provide reasonable protection on the IWSDB. For protection, the DoD suggested that "enforcement will be by a multi-level secure (MLS) trusted computing base (TCB) rated initially at B1 level of trust and progressing to B3 level." [Ref. 7: p. 34] Even though this statement of security policy is ensured on the operating system and telecommunication, the extensive data sharing between contractors, subcontractors, and government activities will introduce legal issues (e.g., proprietary data rights (who owns the data when), sharing licensing, warranties and liabilities, and international data exchange). Thus, consideration on the data rights throughout a product's life-cycle should be done in the early stage of each contract.

III. CALS TELECOMMUNICATIONS PLAN

CALS is intended to automate technical data and drawing deliverables, including technical manuals and CAD/CAM products. During its evolving history, CALS has included many new areas, such as Concurrent Engineering (CE) and Electronic Commerce/Electronic Data Exchange (EC/EDI), to match the advance of Information Technology in the weapon system acquisition processes. To achieve full benefits of these new approaches, real-time on-line data transmission requirements and interoperable telecommunications protocols are very critical. Thus, adequate telecommunications capability, based on open system architecture, must be available, along with neutral data exchange standards. This chapter briefly describes the current situation of CALS data exchange, telecommunications capability, and standards.

A. INTRODUCTION

1. Phased Approach

Automated standardized data coupled with real-time means of access will lower procurement and support costs, increase efficiencies, and result in a greater ability to disseminate and reuse data. To accomplish this, CALS must provide an integrated telecommunications system that can deal with enormous CALS technical data transmission requirements, regardless of the location of those data. The main direction of DoD for the CALS telecommunications architecture is the migration to Open Systems Interconnection (OSI), which is consistent with the overall CALS plan. For full CALS implementation, Doby [Ref. 20] recommended a three phased approach:

- Near Term (1989 - 1990). In the near-term, special attention should be given to the local environment because the bulk of data transfer over geographically dispersed areas will generally be accomplished off line in this timeframe. Usage of DDN should be limited to high-priority/low-bandwidth transmissions.

- Mid Term (1991 -1992). The ability of the DDN to support all the required protocols should become available during the mid term; however, its use should still be restricted to high-priority/low-bandwidth transmissions.

- Long Term (1993 - 1994). The long-term phase will include the addition of the higher bandwidth physical media required to support on-line transfer of bulk file data associated with CALS projects.

Doby also anticipated the utilization of Integrated Services Digital Network (ISDN) for the long-haul connection after 1994. Yet his plan was too optimistic and on-line transmission of the CALS technical data is still not popular. Contributing factors come from several areas: Open System Interchange (OSI) standards, long-haul bandwidth, network security, and trends of industry telecommunication. These reasons will be covered in following sections.

2. Data Delivery Methods

On-line interactive access to the CALS data repository (e.g., IWSDB) is the goal of CALS. This provides immediate and timely data access for custom report generation, document generation, and on-line request of information transmitted as composed products and processable data files. On-line transmission of the full volume of CALS technical data through existing telecommunications architecture is technically feasible, but it is not a cost efficient method because an extremely large amount of data transmission requirements caused by engineering drawings can easily overrun current telecommunication networks in DoD and industry.

It is stated in MIL-HDBK 59B that, in near term, telecommunications may be limited to electronic mail exchange of high priority technical data, or other clearly defined uses such as CITIS access [Ref. 7: p. 16]. Therefore, until full development of the nationwide information infrastructure, both physical delivery and on-line access/delivery will be used in the CALS data transmission.

Physical delivery includes delivery of magnetic disks, magnetic tape, or optical disks used to transfer CDRL items to a government site. Magnetic tape is a mature,

stable technology that is able to handle the large volumes of data typically associated with a major defense system acquisition. MIL-STD-1840B provides a guidance for the use of hard copy forms of physical delivery by standardizing formats for exchange of digital information between DoD and industry.

On-Line Access/Delivery is currently governed by MIL-STD-974 (CITIS). It is a contractor-developed service that provides electronic access to and/or delivery of contractually required Contract Data Requirements List (CDRL) data to users. CITIS is intended to be an efficient, contractually implementable means for providing the government with on-line access to contractor-generated data, Government Furnished Information (GFI), and the electronic transfer of such data. Ultimately, CITIS will replace most contractor delivery of hard-copy information currently required by the government throughout the program life-cycle [Ref. 18]. However, the current insufficient long-haul telecommunications capacity limits the use of CITIS to high priority technical data and EDI.

3. CALS Test Network (CTN)

The CALS Test Network (CTN) was established by the DoD in 1988 to test, evaluate, and demonstrate the interchange and functional use of digital technical information of digital data using DoD's CALS standards. The CTN not only tests and evaluates the CALS standards, but also provides the testbeds for DoD and industry coordination by testing applications of vendors. To demonstrate interoperability of CALS standards, MIL 28000 series of military specification are currently under testing. This tests and demonstrates the movement and interchange of technical data by comparing the transmitted data against received data. The participants of the CTN are various: government, industry, academia, and international.

Yet, the CTN is used as a logical network, where most of interchanges are achieved by means of magnetic tape or optical disk, as required by MIL-STD-1840 [Ref. 5: p.89]. For the real-time on-line delivery test, physical links are achieved using the

DDN and various proprietary networks until the telecommunications capacity is large enough for the CALS technical data transmission.

Test of the on-line CALS data transmission is shown in the CALS Electronic Data Interchange (EDI) Test/Demonstration supported by Air Force CTN. This demonstrated an electronic alternative to the current paper-based Request for Quotation (RFQ) process. RFQs, containing CALS technical data from the Engineering Data Computer Retrieval System (EDCARS), were sent via EDI to potential bidders to determine their capability to receive the RFQs and display the CALS engineering drawings clearly enough to allow bid submission. [Ref. 19: p. 10]

Although there is a limitation on the current networks capacity, the efforts to test and evaluate CALS standards (including new approaches such as EDI and STEP) should be continued, not only between government and industry, but also within industries to accomplish fully automated and integrated CALS environment.

B. DATA EXCHANGE REQUIREMENT

The final goal of the CALS approach is the accomplishment of the IWSDB, which services multiple acquisition and logistic functions. As the IWSDB is a logical multi-weapon system repository, the requirement of CALS data transmission may be various depending on the locations of physical data repository and the types of CALS data related to the phase of weapon systems life-cycle. During the telecommunications planning for CALS, these data transmission requirements may provide a guidance to the decision of physical LAN and WAN types. Furthermore, the comparison between CALS data transmission requirement and physical telecommunications capacity gives the basis for the cost-effectiveness of on-line data delivery, even in the long term. For this reason, Delaura et al. showed intersite data flow requirements [Ref. 20]. To support further research of the data flow analysis targeting a specific weapon system, this section provides basic decision rules required to select CALS data types and related CALS standards based on the CALS Implementation Guide (MIL-HDBK-59B).

1. Technical Manuals

Technical Manuals (TMs) are the operating and maintenance instructions for military technicians. They contain a combination of textual narrative and illustrative graphic images presented in a formal, structured, page-oriented format governed by specific functional standards [Ref. 7: p. 62]. These manuals are one of the biggest burdens in the paper-based weapon system support. The implementation of automated data processing technology offers numerous improvement opportunities in preparation, delivery, storage, distribution, and maintenance of technical manuals. Digital representation of these technical manuals are as follows:

a. Composed Document Image File

This file is a static, formatted presentation of the manual, which can be archived, viewed, and printed only after receipt of the file. Two examples of digitally composed document files are Page Description Language (PDL), such as PostScript, and raster (MIL-R-28002). They provide a two-dimensional image of each manual page. Although these options convert a paper copy of legacy data to a digital one, on-line delivery of large size of raster document image and raster graphics files is not preferable even in the future.

b. Processable Text and Graphics File

For processable text, MIL-M-28001 (SGML) is the guiding CALS standard that governs the Document Type Declaration (DTD) and the Formatting Output Specification Instance (FOSI). A DTD is required to completely and rigorously describe the document's structure and content when FOSI is required for document's formatting.

For processable graphics in a technical manual, MIL-D-28000 (IGES) and MIL-D-28003 (CGM) provides vector representation of graphics. The file size of both

29

standards is smaller than raster. The DoD stated that CGM is more preferable option to IGES because of its relatively small size of graphics file [Ref. 7: p. 66].

c. Interactive Electronic Technical Manual (IETM)

Currently guided by MIL-M-87268, MIL-D-87269, and MIL-Q-87270, an IETM is a computer-based collection of technical information needed for troubleshooting and maintenance of a defense system. It presents interrelated information from multiple sources, tailored to user queries in a hypertext format. Thus, it can be a hypermedia document that permits the end-user to locate any information, such as text, graphics, audio, or computer programs, to present it faster and more comprehensively, regardless of the physical data repository. It has a potential capability to replace all paper-based TMs with less storage requirements.

On the basis of telecommunications planning, however, LAN and WAN capacity should support real-time, on-line data delivery. As it is an emerging approach toward a high-payoff area based on the CALS environment, further revision of IETM specification is anticipated.

2. Technical Data Packages

A Technical Data Package (TDP) is a technical description of the product's design, manufacture, quality assurance, and packaging characteristics adequate for procurement. More specifically, the technical description of an element of TDP consists of all applicable technical data, such as engineering drawings and associated lists, product manufacturing specifications and standards, performance requirements, quality assurance provisions, and packaging detail. The digital, deliverable form options for product drawings and associated lists are as follows:

a. Raster Image Files

Raster Image files provide a representation of digitally scanned paper drawings or aperture cards. Guided by MIL-R-28002, it is not a machine intelligible format, and the data can't be processed within a raster image. As mentioned earlier, the large file size of this option makes the on-line delivery uneconomical.

b. CAD Data Files

These files consist of vector data with geometrically accurate and precise representations of the product, together with associated annotations (e.g., dimensions and tolerance). To make them processable in future usage, MIL-D-28000 (IGES) should be used. Subsets of IGES will specify dimensions of CAD data.

c. Product Data Files

In addition to CAD data files, product data files are another processable files in the TDP category. It is more complete and flexible delivery option and also provide a methodology for linking CAE and support processes. Depending on the characteristics of product, the DoD showed various options of standards for product data files: SGML for non-graphic data, VHDL for digital functional design, EDIF for circuit performance description, and EDIF/IPC/IGES for manufacturing data package [Ref. 7: p. 70].

ISO 10303, also known as STEP, is one possible option in this category. Although it is an emerging standard in industry, its powerful technical structure and ability to create and define data models make STEP more capable of putting together all the aspects of product data in a shared database environment with a relatively small file size.

3. Logistic Support Analysis Records (LSAR)

Logistic support analysis builds upon data from related systems engineering and design analysis, and produces a consolidated and integrated set of logistics-related technical data. The resulting LSAR is a logically integrated database consisting of both the engineering source data upon which analysis tasks are based, and the analysis results. The total set of data elements making up an LSAR database is defined by MIL-STD-1388-2. Because of the range of data that can be documented in an LSAR, the LSAR is able to satisfy the data requirements of a number of the deliverables commonly appearing on a Contractor Data Requirements List (CDRL), such as Provisioning Lists and Failure Modes, Effects, and Criticality Analysis (FMECA) reports. On-line interaction between the government and contractors enables more accurate LSAR data. LSAR data can be delivered as LSAR reports or LSAR data files:

a. LSAR Report Image Files

These files are the digital equivalent of the LSAR data in hard copy, and can't be updated or processed further after delivery. The delivery of LSAR reports in the image file format is guided by MIL-STD-1388-2.

b. LSAR Data Files

The basic format used for LSAR data files is alphanumeric. Because it is a processable format guided by MIL-STD-1388-2, the on-line delivery of the LSAR data files can be only changed data tables (showing the difference from the previous submittal of the LSAR data), thus may reduce on-line transmission requirements.

The DoD showed another delivery option for the LSAR data files, ISO 10303 (STEP) [Ref. 7: p. 73]. The capability to describe all the aspects of product data enables the use of STEP even in the LSAR data delivery. However, the use of this integrated data file is a future option presently under development.

4. Training Products

Most of the training products contain a combination of textual narrative and illustrative graphic images presented in a formal, structured, page-oriented format. MIL-STD-1379 contains detailed guidance for delivery of Interactive Courseware (ICW) and other specific training deliverables. The LSAR database shall provide source data to ICW for producing output reports and instructional materials [Ref. 8: p. 8-11].

a. Document Image File

This file consists of composed page images of the full training product. Each page image represented by a two-dimensional image is guided by MIL-R-28002 raster standard or Page Description Language (PDL). The impact of document image files on long-haul on-line delivery is the same as technical manuals.

b. Processable Data File

The processable data file is composed of one set of files for textual data, and a separate set of graphic illustrations or drawings. At present, the format of text file is defined by MIL-M-28001 (SGML) with appropriate DTDs, and the graphics format is defined by MIL-D-28000 Class I subset or MIL-D-28003 CGM. For training purposes, CGM is more a preferable option than IGES.

c. Future Options

As the range of training products is not limited in paper-oriented tutorials, the multimedia, such as video and audio clips, and/or pageless training products will soon appear in this category. However, to support these options, additional data sets in the LSAR database, large bandwidth in the networks, and appropriate software tools are also required.

5. EC/EDI

EDI is the intercompany, computer-to-computer exchange of business documents in standard electronic data formats. These electronic transactions include invoices, shipping schedules, advance ship notices, court filing, bills of lading, and purchase orders. Rather than E-mail, which can use free-formatted message-length unit, EDI uses predefined, fixed-format message-length units known as EDI transaction sets. The Federal Information Processing Standard (FIPS) 161, published by NIST in 1991, suggests the use of either UN/EDIFACT or the ANSI ASC X12. The global use of Internet promotes EDI as one of the best solutions to replace paper-based business transactions. The actual size of an EDI message varies depending on transaction sets. Yet, the relatively small size of EDI messages are allowable even through the current commercial Internet.

C. CALS TELECOMMUNICATIONS STANDARDS

1. International Standards (OSI)

If different vendors use different data formats and data exchange conventions, the communication among these heterogeneous machines will be extremely difficult. To avoid this problem, and to give a common set of conventions in the software development, the International Organization for Standardization (ISO) established a subcommittee to develop an architecture in 1977. The result was the Open Systems Interconnection (OSI) reference model, adopted by ISO in 1983, which is a framework for defining standards for linking heterogeneous computers. The purpose of this effort is to provide a common basis for the coordination of standards development for the purpose of systems interconnection, while allowing existing standards to be placed into perspective within the overall Reference Model [Ref. 21: p. 437].

34

Table 5. OSI Reference Model

Layer	functions and capabilities
Application Layer	Allows for protocols and services required by particular user-designed application processes. Functions satisfying particular user requirements are contained in this layer. Representation and transfer of information necessary to communicate between applications are the responsibility of the lower layers.
Presentation Layer	Specifies or, optionally, negotiates the way information is represented for exchange by application entities. It provides the representation of: 1) data transferred between application entities, 2) the data structure that the application entities use, and 3) operations on the data's structure. This layer is concerned only with the syntax of the transferred data. The data's meaning is known only to the application entities.
Session Layer	Allows cooperating application entities to organize and synchronize conversation and to manage data exchange. To transfer the data, session connections use transport connections. During the session, session services are used by application entities to regulate dialogue by ensuring an orderly message exchange on the session connection.
Transport Layer	Connection-oriented service provides reliable, transparent transfer of data between cooperating session entities. The transport layer entities optimize the available network services to provide the performance required by each session entity. Optimization is constrained by the overall demands of concurrent session entities and by the quality and capacity of the network services available to transport layer entities. In the connection-oriented transport service, transport connections have end-to-end significance, where the ends are defined as corresponding session entities in communicating end systems. Connection-oriented transport protocols regulate flow, detect and correct errors, and multiplex data, on an end-to-end basis.
Network Layer	Provides message routing and relaying between end systems on the same network or on interconnected networks, independent of the transport protocol used. The network layer may also provide hop-by-hop network service enhancements, flow control, and load leveling. Services provided by the network layer are independent of the distance separating interconnected networks.
Data Link Layer	Provides communication between two or more (multicast service) adjacent systems. This layer performs frame formatting, error checking, addressing, and other functions necessary to ensure accurate data transmission between adjacent systems.
Physical Layer	Provides a physical connection for transmission of data between data link entities. Physical layer entities perform electrical encoding and decoding of the data for transmission over a medium and regulate access to the physical network.

The OSI Reference Model uses seven functional layers. The functions and capabilities expected at each layer are specified in the reference model. However, the model doesn't prescribe how this functionality must be implemented. Table 5 shows the general services provided by each layer in the reference model.

2. GOSIP

Government Open System Interconnection Profile (GOSIP) is based on agreements reached by vendors and users of computer networks participating in the National Institute of Standard and Technology (NIST) Workshop for Implementors of OSI. It defines a common set of OSI data communication protocols that enable systems developed by different vendors to interoperate and enable the users of different applications on these systems to exchange information via communication links. Based on the International Standards Organization OSI reference model, GOSIP has been designated Federal Information Processing Standard (FIPS) 146 in 1988. The new version of GOSIP (FIPS 146-1) was published in April 1991 to provide a remote terminal access capability and extended interoperability [Ref. 22]. GOSIP mandates that government agencies, when acquiring computer networking products, purchase OSI capabilities in addition to any other requirements.

CALS adopted GOSIP as a future standard for telecommunications media access and delivery standards. Another reason of this adoption was that GOSIP was consistent with, and complementary to, industry's Manufacturing Automation Protocol (MAP) and Technical Office Protocol (TOP) which adopted OSI protocols. MIL-STD-1840B states that "GOSIP will be able to interoperate with the DoD protocols; it is therefore, encouraged that acquisitions of telecommunication products require the delivery of systems that satisfy the data communication protocol specifications of GOSIP."

3. TCP/IP

Before OSI reference model and protocol suites were developed, Transmission Control Protocol and Internet Protocol (TCP/IP) provided the only practical method for computers from different manufacturers to communicate. TCP/IP were originally developed as part of the Advanced Research Projects Agency Network[5] (ARPAnet) in the

---

[5] An experimental network designed to support military research to build networks that could withstand partial outages (e.g., bomb attacks) and still function.

early 1970s. Compared to the complex OSI protocol suite, the TCP/IP protocol suite is relatively simple, hence provides easy interoperability among heterogeneous computers.

At present, TCP/IP is the most favorite protocols in industry and government. Olsen showed the result of a survey presenting the dominance of TCP/IP over OSI [Ref. 23]. As large, heterogeneous networks have grown up over the past several years, the leading mainframe, midrange, and microcomputer vendors all have been forced to incorporate TCP/IP into their product offerings. The explosive growth of commercial Internet connections also largely contributes to the growing population of TCP/IP stacks.

Although CALS adopted GOSIP as a strategy promising ubiquity above various communication hardware and software, in reality, it had partially supported the proliferation of TCP/IP by mandating the DDN compatibility for its intermediate step. As the DDN is based on TCP/IP, the contractor should provide the appropriate number of DDN interfaces for each host, node, or LAN in addition to OSI suite [Ref. 13: p. 179]. The result is that TCP/IP are still used when GOSIP is not.

Quarterman stated that "GOSIP never required anyone to actually use OSI, just to procure it. Most every vendor also supplies TCP/IP, and that is generally what is actually used." [Ref. 24] Now GOSIP is not a mandatory specification in acquisitions of products and services for communications between dissimilar computer systems. According to the recommendations of the final report of the Federal Internetworking Requirements Panel (FIRP), dated May 31, 1994, GOSIP was renamed to the Profiles for Open Systems Internetworking Technologies (POSIT), and mandatory compliance to OSI was changed to strong encouragement to "open voluntary standards." [Ref. 25]

In spite of TCP/IP's strength as a transport protocol, the OSI model's application layer X.400 message handling service and X.500 directory service protocols are gaining in popularity. The current trend of E-mail software vendors is to interface two different protocols together. On the basis of CALS telecommunications planning, the selection decision between two different protocol suites should reflect the interoperability to integrate islands of automation.

4. Multiprotocol Interoperability

Instead of selecting one protocol suite as a dominant telecommunications protocols, the use of gateway gives interoperability between OSI and TCP/IP. As mentioned earlier, the communication gateway option in the CALS telecommunications plan was intended to convert TCP/IP protocols to GOSIP protocols for a limited time period required for migration from TCP/IP to OSI protocols. Now the situation is changed. The TCP/IP protocols are widely used for the internetworking; hence, they may provide the most promising interoperability option. However, the same gateway option presented in the CALS telecommunications plan will be used to support partial OSI applications, such as X.400 and X.500 protocols.

Gateways can be grouped in various ways. A common general grouping scheme uses the attributes on which the gateway sevices operate: an address gateway, a protocol gateway, and a format gateway. [Ref. 26: p. 420]

- Address Gateway: Connects networks that have different directory spaces but that use the same protocols. This type of gateway is common, for example, when dealing with a Message Handling Service (MHS).

- Protocol Gateway: Connects networks that use different protocols. This gateway does the protocol translations.

- Format Gateway: Connects networks that use different representation schemes (e.g., ASCII versus EBCDIC). The gateway maps between the two formats.

To support X.400 with TCP/IP protocols, a protocol gateway can be used. An example of the gateway function to translate OSI protocols to TCP/IP protocols is shown in Figure 6.

The use of ISO Development Environment (ISODE) software provides another option without using a gateway to translate different protocols. By locating an ISO transport level protocol interface on top of TCP/IP, higher-level OSI protocols can be directly used like other TCP/IP applications [Ref. 27: p. 494].

OSI Layer	OSI Protocols	TCP/IP Protocols
Application	X.400	SMTP
Presentation	ASN.1	
Session	ISO Session Protocol	TCP
Transport	TP4	
Network	CLNP	IP

Figure 6. E-Mail Gateway between OSI Protocols and TCP/IP Protocols

Although this thesis only reviews TCP/IP and OSI protocols for the interoperability of CALS telecommunications, there are also other protocols already developed and used at present. Thus, the enforcement of using TCP/IP with gateway options can not provide an ubiquitous solution for the all the areas of internetworking. In the long-term telecommunications plan for interoperability, a unique way to solve those multiprotocol networks should be provided to meet diverse user requirement. For this reason, Clark suggested that the next generation Internet Protocol (IPng) should have features that support its use with a variety of protocol architectures [Ref. 28]. So, it would be wise to keep up with new approaches to enable the maximum interoperability for the CALS telecommunications plan.

D. CALS NETWORK INFRASTRUCTURE

To support various CALS-related strategies, connectivity between government and industry and within government agencies is essential. This connectivity is achieved from

intrasite and intersite connection. In the beginning of the CALS telecommunications plan, CSMA/CD, which has a 10 Mbps capacity, was recommended for the intrasite connection. At present, FDDI is one of the popular options for the LAN. It gives 100 Mbps bandwidth with a high level of reliability. Although more bandwidth promises faster data transmission, a 10 Mbps to 100 Mbps capacity might be sufficient for CALS data transmission.

The bottleneck comes from long-haul connectivity, which supports intersite data transmission. This is one reason why MIL-STD-1840 is providing off-line CALS data delivery. Although new technologies such as STEP promise less transmission requirements, the minimum capacity required by CALS data transmission on the intersite connection should be provided. However, CALS strategy doesn't intend to install new network infrastructure; Currently available network infrastructure and near-term deployment of new infrastructure should be analyzed to enable on-line transmission of CALS technical data.

1. DDN

Operated by the Defense Information Systems Agency (DISA), the DDN is a packet-switched network designed to provide DoD with reliable, survivable, and secure worldwide communications. Established in 1982 as the DoD common-user data communications network, the DDN was based on ARPAnet packet-switching technology. The DDN enables computer systems and terminals/workstations acquired from different manufacturers to exchange information by using TCP/IP protocols. It currently offers a maximum user data rate of up to 56 Kbps. Based on the levels of security, the DDN currently consists of four separate networks; MILNET for unclassified communications, and DSNET 1-3 for classified communications. For CALS use of DDN, Delaura et al. assessed that the daily volume of intersite CALS data transmission would saturate the entire DDN, but DDN can provide partial CALS support [Ref. 20: p. 2-8].

2. DCTN

The Defense Commercial Telecommunications Network (DCTN) is a satellite-based network that is used primarily for voice and video. It is a service that provides many major military locations with T1 (1.544 Mbps) transmission speeds. Managed by DISA (formerly DCA), the DCTN contract was awarded to AT&T in March 1984. The service provides support for both dedicated and switched facilities, and can be reconfigured dynamically from a network control center. All transmissions and switching are digital. DCTN terrestrial links support switched voice, dedicated voice and data, and video conferencing. The bandwidth is divided into 24 voice channels of 56 Kbps each. Dynamic allocation of bandwidth is used to support video conferencing [Ref. 20: p. 2-8].

The CALS community has been interested in DCTN, especially its general properties of satellite networks. However, before DCTN was analyzed for CALS data transmission, the focus of CALS telecommunications moved toward better service, such as FTS-2000 or DISN.

3. DISN

In June 1993, the Chairman of the Joint Chiefs of Staff (CFCS) ordered the establishment of the Defense Information System Network (DISN) with the original objective to achieve a single DoD worldwide common user IP router network. The CJCS directed all DoD Service/Agencies to use the DISN as the primary WAN for all DoD long-haul common-user telecommunications services. Currently, the DISN data service is composed of 86 hub routers, formerly the Defense Logistics Agency Corporate Network (DCN), and ten routers that provide the interconnection service for the DoD and non-DoD router network, formerly the DDN pilot Internet. [Ref. 29: p. 40]

At present, DISA plans evolutionary development of new DISN which is a global mega-network capable of handling voice and high bandwidth data such as imagery. It is envisioned as DISA operated and managed network running on DoD-owned switches

with pipes acquired competitively. DISA expects to end up with a Synchronous Optical Network (SONET) running on advanced Asynchronous Transfer Mode (ATM) switches [Ref. 30: p. 37]. It is anticipated that, after the completion of DISN, it will give much more flexibility to the on-line CALS data transmission.

4. FTS-2000

Federal Telecommunications System 2000 (FTS-2000) was established in December 1988 to provide long-haul communications for all government agencies. Managed by General Services Administration (GSA), FTS-2000 consists of two major contracts with AT&T and U.S. Sprint. Packet switched services for data transmission provides 56/64 Kbps dynamic connectivity. Dedicated transmission service for point-to-point private line services provides T1 (1.544 Mbps) connectivity. It also provides video transmission service for compressed video and full motion teleconferencing. The FTS-2000 backbone consists of switches that are interconnected by T3 (44.7 Mbps) fiber-optic links. The DoD plans call for using the FTS-2000, with the CALS network as one of the likely major users [Ref. 2: p. 8]. The FTS-2000 contracts are due to expire in December 1998.

5. Commercial Internet

The Internet is the inter-networking of existing corporation and government networks using common TCP/IP protocols. Krol states that it was born out of an effort to connect a U.S. Defense Department network called the ARPAnet and various other radio and satellite networks [Ref. 31: p. 13]. Grown from NSFNET, originally commissioned by the National Science Foundation (NSF), the Internet provides an international-wide academic network. Recently, many corporations also take part in the Internet to have their nationwide corporate network. Now it becomes a network of networks connected by more than 40,000 networks and 4 million host computers around the world.

At a recent meeting in Toronto, Canada, the Internet Engineering Task Force (IETF) made a decision that could make the Internet the backbone of the information superhighway [Ref. 32]. To support global use of the Internet, and to overcome the limitation on its current addressing structure, IETF is going to suggest a "next generation" Internet protocol (IPNG).

Actually, the Internet provides the widest connectivity at less cost. Federal agencies and even military agencies use the Internet for their operations as an efficient and effective means of communication and information distribution [Ref. 33]. The EDI using the Internet is a hot issue at present. However, the decision to use the commercial Internet in CALS data transmission is not clear, because CALS technical data are not only extremely large, but they also include large portions of classified information. With more than current bandwidth provided by military networks, appropriate data protection methods should be developed and adapted. The Multilevel Information Systems Security Initiative (MISSI), sponsored by the National Security Agency (NSA) suggests one possible solution for the transmission of classified data through the public Wide Area Network (WAN).

E. SUMMARY

CALS is an extremely long-term project requiring a great deal of effort and money. Although the DoD carefully planned the phases of CALS telecommunications architecture, it was already overdue. Some of the plans are not matched with the current situation of telecommunications trends. To accomplish a successful CALS environment, timely and adequate alterations are important to overcome unexpected obstacles located on the way to automation and integration of infomation. However, the changes sometimes bring much more difficulties and registrations than the original situation. Thus, the initiation of the CALS telecommunicaions plan should be flexible enough to overcome any unpredicted difficulties.

At present, the Defense Ministry (MND) of Korea is trying to proliferate CALS with the cooperation of industry. The effort to implement CALS was begun much later than in the U.S., but the later start gives an advantage. On the basis of CALS telecommunications planing, the history of the United States approach shows some of the very important factors for successful CALS implementation.

First of all, the network blueprints should be flexibly prepared. Networks are the fundamental infrastructure to implement CALS. However, it may not be separately constructed for the CALS implementation only. Currently the Korean MND is implementing a Ministry-wide computer network. It consists of backbone with T1 capacity and other branching lines. It is far behind CALS data transmission requirements. The rapid proliferation of the commercial Internet gives one possible solution, but it should be equiped with appropriate network security policy and methodologies. The National Information Infrastructure (NII) is another solution, yet it is too far. The law of economics suggests using current infrastructure, and providing bridges that connect the present situation with the future one.

Second, the capacity required for the on-line data traffic should be analyzed. The network capacity depends on the weakest bottleneck of data transmission. In other words, insufficient capacity at one place in a network can impact entire network's capacity, and may require revision of the telecommunicational strategy. So, on-line data transmission and the actual location of the data should be carefully analyzed and designed.

Third, the end user requirement should not be underweighed. Although CALS is a global strategy to enhance the information flows between the government and industry, the success of this approach may depend on the hands of end users who actually deal with it. Without a careful consideration of user requirements, the expensive investment on CALS implementation shall not pay off.

Fourth, the direction of CALS implementation should be exact and specific. CALS can improve processes using information technology. But, too broad a scope results in poor management of the entire project. At present, the U.S. CALS strategy is returning to

its original goal, logistics support. It was criticized by Congress for spending 10 years and $ 5 billion and not showing any results. As a consequence, the Government Information Enhancement is moving to Enterprise Integration (EI), which promised tighter management of the automation and integration of information.

IV. NETWORKS SECURITY AND RELATED ISSUES

In reality, CALS still prefers courier services to on-line data transmission. The reason for this preference is not only the extremely large file size for engineering drawings, but also the lack of security in networks carrying CALS technical data. The major concern about CALS data protection during the transmission is data encryption. As CALS technical data travel on the unsecured communication media, the data should be secure enough to protect themselves. However, the CALS implementation guide (MIL-HDBK-59B) and on-line information service guide (CITIS) still do not specify details of the encryption devices or software.

At present, MIL-STD-1840B, which describes delivery methods of CALS data in magnetic tapes or optical disks, is the only option for the classified data delivery in digital format. According to the Tomlinson, the Army's JCALS program manager, about 10 percent of CALS-related information is classified [Ref. 34]. He was considering another island of information by removing the 10 percent of information to a separate JCALS workstation to control access to secure data. Thus, without adequate support of classified data transmission, a fully integrated CALS environment is still far away.

As part of an effort to propose a secure CALS telecommunications architecture, this chapter analyzes the roles of network security and the ways of data protection in the CALS environment.

A. INTRODUCTION

1. Impact of Networks Security

To accomplish a highly integrated CALS environment, internetworking among distributed systems, and the use the networks and communications facilities for carrying data are one of the basic requirements of the CALS implementation. But, when the range of systems has expanded, the vulnerability of the data transmitted among systems has also increased.

The term "network security" refers to protection against any unauthorized modification, disclosure, and destruction of network information, or loss of network service leading to the non-availability of critical information. Thus, the security issues that are raised regarding networks are more complex than conventional computer systems. The reasons for these increased security issues inherent in networks were shown by Pfleeger [Ref. 35: p. 372].

- Sharing. Because of the resource and workload sharing of networks, more users have the potential to access networked systems than single computers. Thus, access controls for single systems may be inadequate in networks.

- Complexity of System. A network operating/control system is likely to be more complex than an operating system for a single computing system because a network combines two or more possibly dissimilar operating systems with mechanisms for interhost connection. Thus, the certification of a network is more difficult than a single computing system.

- Unknown Perimeter. The expandability of a network brings uncertainty about the network boundary. One host may be a node on different networks, so that resources on one network are accessible to the users of other networks as well. Although wide accessibility is an advantage, the unfixed boundary of networks may allow unintentional connection to potentially malicious users.

- Many Points of Attack. When a file is shared by several different networks, it may pass through many different nodes from source to destination. Thus, the weakest point of nodes gives the best chance to disclose the secrecy of data. The enforcement of the access control mechanisms over all those networks is more difficult than a single computing system.

- Unknown Path. Especially in packet-switching networks, there may be many paths from one host to another, as network users seldom have control over the routing of their messages. To cover all the possible paths by security mechanisms is not an easy task.

As a result, networks make data more vulnerable to any potential threat than a single computing system. Privacy of data, data integrity, and authenticity of data are typical examples of the vulnerability expanded by networking. First, as mentioned

above, with many unknown users on networks, concealing sensitive data becomes more difficult. Second, because more nodes and more users have potential access to a computing system, the risk of data corruption is higher. Third, it is more difficult to assure the identity of a user on a remote system. To protect these vulnerabilities, adequate countermeasures should be employed.

2. Security Attack

A security attack is defined as any action that compromises the security of information owned by an organization [Ref. 36: p.4]. It can be any action that threatens privacy, integrity, and authenticity of data. The types of attack can be categorized into passive attacks and active attacks.

a. Passive Attacks

A passive attack is any action of eavesdropping on, or monitoring of, a transmission. It is called a passive attack because it is done without interfering with the data flow. The most fundamental type of passive attack is the "release of message contents". Another type of the attack is "traffic analysis". This type of the attack intends to obtain not the contents of message but other information useful in guessing the nature of the communication. Packet headers, for example, gives adequate information regarding the location and identity of communicating hosts. The length and frequency of messages provide the pattern of messages being exchanged.

Passive attacks are very difficult to detect since they do not involve any alteration of the data. However, it is feasible to prevent the success of these attacks by isolating a network or using cryptosystems. Thus, the emphasis in dealing with passive attacks is on prevention rather than detection [Ref. 36: p. 8].

b. Active Attacks

An active attack, called active wiretapping, is any action related to interruption, modification, or fabrication of data. It can be subdivided into four categories: masquerade, replay, modification, and denial of service [Ref. 36: p. 9].

A "masquerade" takes place when one entity pretends to be a different entity. It usually includes one of the other forms of active attack. "Replay" involves the passive capture of a data unit and its subsequent re-transmission to produce an unauthorized effect. "Modification of message" means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect. The "denial of service" prevents or inhibits the normal use or management of communications facilities. It can be the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

An active attack has the opposite characteristics of passive attack. It can be easily detectable, but difficult to prevent since the prevention means protection of entire networks. Thus, the emphasis in dealing with this attack is on detection and the recovery of data disrupted or delayed. The stalling states that the detection may also contribute to prevention because, the detection has a deterrent effect [Ref. 36: p. 10].

3. Security Service and Mechanism

Security Service is a service that enhances the security of the data processing systems and the information transfers of an organization. Its actual role is to provide countermeasures against security attacks by using security mechanisms designed to detect, prevent, or recover from security attacks. Although many characteristics used in security service come from paper-based document protection, the nature of digital bits make the service more difficult. To provide security services, encryption acts as the most common means. However, encryption itself is not enough to provide all the services, so combination of other techniques and devices with encryption mechanisms are used to provide the security services. Stalling suggests one useful classification of

50

security services useful in network security: Confidentiality, Authentication, Integrity, Non-repudiation, Access Control, and Availability [Ref. 36: p. 10-12].

a. Confidentiality

This service is used to protect transmitted data from passive attacks. With respect to the release of message contents, several levels of protection can be identified. The protection mechanisms supporting this service are based on cryptographic techniques. In a network environment, link-to-link or end-to-end encryption can be provided.

b. Authentication

This service is concerned with assuring that a communication is authentic. In the case of a single message, the function of authentication service is to assure the recipient that the message is from the source that it claims to be from. In the case of an ongoing interaction, the function is to assure that the two communication entities are authentic, and the connection is not interfered by a third party who can masquerade as one of the two legitimate parties for the purpose of unauthorized transmission or reception. The protection mechanisms can be simple password schemes or cryptographic techniques attached in the hardware device, such as a token or smart card.

c. Integrity

This service provides proof of the integrity of data in the communication and can be used to detect and protect against the manipulation and modification of data. It is a service related to active attacks; thus, the detection mechanisms are used to provide the service. Integrity mechanisms employ cryptographic techniques to produce integrity checksums, which can be used to determine whether there has been any insertion, deletion, or reordering of the original sequence of messages.

d. Non-repudiation

Non-repudiation prevents either sender or receiver from denying a transmitted message. It is a service to prove the origination and destination of a message to the receiver and sender, respectively. Digital signature mechanisms and/or one-way hashing functions are used to provide the non-repudiation service.

e. Access Control

Access control is the ability to limit and control the access to host systems and applications via communications links. Combined with authentication service, access control can be tailored to each of the access grants, depending on the classification of data and user to protect against the unauthorized use of resources. Discretionary access control and mandatory access control are the examples of this service.

f. Availability

A variety of attacks can result in the loss of or reduction in availability. Denial of service is usually regarded as an extreme case of these attacks. Thus, availability services are congregated services, including authentication, encryption, and other adequate physical actions to provide a seamless communications environment between two entities.

B. FUNDAMENTALS OF DATA ENCRYPTION

1. Introduction

Encryption is a means of maintaining secure data in an insecure environment. It is the process of changing a message called plaintext to ciphertext. In a networked environment, encryption allows secure communication over an insecure channel. By

using encryption, the plaintext is disguised so that, even if the transmission is diverted, the message will not be revealed. Most of the security mechanisms used in networks are based on the data encryption, whether those mechanisms are provided by applications software or embedded in hardware devices.

With respect to decrypting the encrypted message, encryption techniques can be divided into two categories: symmetric key cryptography and asymmetric key cryptography. In a symmetric cryptosystem (also called private key, single key, secret key, or conventional cryptosystem), both the encryption and decryption transformation use the same key. The security of the encryption method is dependent on the robustness of encryption algorithm. On the other hand, in an asymmetric key cryptosystem (also called public key cryptosystem), a pair of keys are used to encrypt and decrypt a message. By encrypting and decrypting with a separate key, asymmetric key cryptography provides a better way to distribute and manage the keys than conventional cryptography. However, the transformation speed using asymmetric key cryptosystem is much slower than conventional cryptosystem, because of its complicated mathematical algorithm.

For encryption, the best solution is to combine symmetric and asymmetric key systems in order to get both the security advantages of asymmetric key cryptography, and the speed advantages of symmetric key cryptography. For example, asymmetric key cryptography can be used to encrypt a secret key, which is then used to encrypt the bulk of a file or message. Fahn suggested that public key cryptography is not meant to replace secret key cryptography, but rather to supplement it, and to make it more secure [Ref. 37: p. 6].

The hashing function, also called message digest, is used as another means to assure the integrity of a received message. Usually combined with other cryptosystems, it usually supports data integrity by providing evidence whether the original message transmitted is altered or not. It is similar to symmetric cryptography because it uses the same scheme to produce a hashed message at sender's and receiver's computers, but the

53

difference is that the result of hashing is independent to the length of the original message.

2. Secret Key Algorithm

Secret key cryptography involves the use of a single key that is mutually shared by two communicating entities. Given a message and the key, encryption produces unintelligible data that is about the same length as the plaintext was. Decryption is the reverse of encryption, and uses the same key used for encryption [Ref. 37: p. 45]. One major advantage of using a secret key algorithm is fast encryption speed, so large files can be quickly transformed to a cipher text and networks can transmit that file without any performance degrading. However, with a secret key algorithm, the key should be pre-exchanged before encryption, whether using a courier service or another key distribution technology.

a. Data Encryption Standard (DES)

Data Encryption Standard (DES) was published in 1977 by the National Bureau of Standards for use in commercial and unclassified U.S. Government applications. It was based on an algorithm known as the "Lucifer" cipher designed by IBM in 1974. DES uses a 56-bit key, and maps a 64-bit input block into a 64-bit output block. The key actually looks like a 64-bit quantity, but one bit in each of the 8 bytes is used for odd parity on each byte. Therefore, only 7 of the bits in each byte are actually meaningful as a key [Ref. 38: p. 60]. DES uses a substitution technique and a transposition technique, and these two techniques are repeated for 16 cycles, one on top of the other. The same key used in encryption is also used in decryption, but in the reverse order. DES can be efficiently implemented in hardware, but is relatively slow if implemented in software.

A powerful technique for improving the security of DES is multiple encryption, that is, encrypting each message block under several different DES keys in succession. Triple encryption is thought to be equivalent to doubling the key size of DES

succession. Triple encryption is thought to be equivalent to doubling the key size of DES to 112 bits [Ref. 37: p. 37]. It can actually prevent any decrypting attempt, although it takes three times longer than single-encryption DES. Triple DES has been adopted for use in the key management standards ANSI X9.17 and ISO 8732, and for Privacy Enhanced Mail (PEM) [Ref. 36: p. 67].

b. International Data Encryption Algorithm (IDEA)

IDEA is a new block-oriented, conventional encryption algorithm developed by Lai and Massey of the Swiss Federal Institute of Technology [Ref. 38: p. 74]. IDEA uses a 128-bit key to encrypt data in blocks of 64 bits. It has 17 rounds to encrypt each of 64 bits of message block. The 126-bit key is divided by 52 of 16-bit sub-keys, whereas the message is divided into four 16-bit sub-blocks during the operation. Like DES, IDEA uses a complicated mangler function that does not have to be reversible for decryption.

IDEA is designed to facilitate both software and hardware implementation. Hardware implementation, typically in VLSI, is designed to achieve high speed, while software implementation has the advantage of flexibility and low cost. Currently, IDEA is used in Pretty Good Privacy (PGP), one of the secure e-mail applications.

c. RC2 and RC4

RC2 and RC4 are another type of well-known secret key cryptosystems. They are variable-key-size symmetric block cipher functions for fast bulk encryption. They are as fast or faster than DES. As they use variable key sizes, the comparison to DES in terms of strength depends on the key size.

RC2 can be used in same modes as DES, including triple encryption. It is approximately twice as fast as DES, at least in software. RC4 is a variable-key-size symmetric stream cipher, and is 10 or more times as fast as DES in software. Both RC2

and RC4 are very compact in terms of code size. RC2 and RC4 have been widely used by developers who want to export their products [Ref. 37: p.49].

3. Public Key Algorithm

The first public key cryptography was invented in 1976 by Diffie and Hellman in order to solve the key management problem in secret key cryptography [Ref. 36: p. 109]. In this system, each person or communicating entity gets a pair of keys, called the public key and private key. Each person's public key is published or often posted on electronic bulletin boards, while the private key is kept secret. The need for sender and receiver to share a unique secret key is eliminated. All communications involve only public keys, and no private key is ever transmitted or shared.

Currently available public key cryptosystems provide two additional applications: encryption/decryption and digital signature. In encryption/decrytion, the recipient's public key is used to encrypt a message by a sender so that only the recipient can decrypt the message with his/her own secret key. In digital signature, the sender's private key is used to sign a message so that the recipient can verify the identity of the sender by decrypting the message with the sender's public key. Signing is achieved by a cryptographic algorithm applied to the message or to a small block of data that is bound in some way to the message [Ref. 36: p. 114]. At present, four public key cryptosystems are available, yet the use of those cryptosystems depends on their capability to serve applications. Table 6 shows those cryptosystems and their capability.

Table 6. Applications for Public Key Cryptosystems [Ref. 36: p. 115]

Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Yes; impractical for large blocks	Yes	Yes
LUC	Yes; impractical for large blocks	Yes	Yes
DSS	No	Yes	No
Diffie-Hellman	No	No	Yes

Public key cryptosystems are based on the trap-door one-way functions [Ref. 37: p. 30]. The public key gives information about the particular instance of the function. The private key gives information about the trap door. Whoever knows the trapdoor can perform the function easily in both directions, but anyone lacking the trap door can perform the function only in the one direction, usually for encryption. The strength of those functions comes from the complexity of the mathematical computation, such as the discrete logarithm and modular exponential algorithm.

a. RSA

RSA is named after its inventors, Rivest, Shamir, and Adleman. RSA has two important functions not provided by DES: secure key exchange without prior exchange of secrets, and digital signatures. The key length is variable. Anyone using RSA can choose a long key for enhanced security, or short key for efficiency. The most commonly used key length for RSA is 512 bits. The encryption block size in RSA is also variable. The plain text block must be smaller than the key length. The encrypted block will be the length of key. [Ref. 38: p. 134]

The premise behind RSA's security is the assumption that factoring a big number is very difficult. The best known factoring methods are really slow. To factor a 512-bit number with the best known techniques would take about a half million MIPS-year [Ref. 38: p. 135]. Even though a new factoring algorithm may be developed in the future, the extension of key size will make the security of RSA more robust. In fact, the weakness of RSA is found not from the algorithm, but from the poor management of the secret key, which is the same problem considered in other public key algorithms.

RSA is much slower than any secret key algorithm. To encrypt a message, RSA is combined with a secret key algorithm, such as DES, by means of an RSA digital envelope. For encrypting messages, the message is first encrypted with a random DES key, and then, before being sent over an insecure communications channel, the DES key

is encrypted with RSA. Together, the DES-encrypted message and the RSA-encrypted key are sent [Ref. 37: p. 9].

To release the burden of the actual RSA implementations in different situations, RSA provides the Public-Key Cryptography Standard (PKCS) and other helpful guides [Ref. 38: p. 145]. Composed of a set of standards, PKCS defines the encodings for things such as encryption and digital signing to help the software industry actually implement RSA into their applications.

b. Digital Signature Standard (DSS)

The Digital Signature Standard (DSS) was proposed by NIST in cooperation with the NSA as draft FIPS PUB 186 in 1991. In 1994, the U.S. Commerce Department approved the DSS as the mandatory standard for agencies using digital signature applications. The algorithm of the DSS is known as Digital Signature Algorithm (DSA). The DSA is based on the difficulty of computing discrete logarithms, and it is based on schemes originally presented by ElGamal and Schnor. [Ref. 36: p. 344]

The DSA provides signature generation and verification. Simply, signature generation is done with a sender's private key, and verification is done with a sender's public key by a recipient. The keys are generated by logarithmic manipulation of two large prime numbers, which are 160-bits and 512-bits long. The signing and verifying procedure uses another algorithm, Secure Hash Standard (SHS), to generate a condensed version of data called message digest.

The DSA authenticates the integrity of the signed data and the identity of the signer. The DSA may also be used to prove to a third party that data was actually signed by the generator of the signer (signature certification). Although the DSS cannot be used for encryption or key exchange, it can be used for other applications which require data integrity assurance and data origin authentication.

4. Hash Function and Message Digest

A hash function is a computation that takes a variable-size input and returns a fixed-size representation of input, which is called hash value. If the hash function is one-way (i.e., hard to invert), it is also called a message-digest function, and the result is called a message digest [Ref. 37: p. 47]. A hash function can usually serve to detect modification of a message. For digital authentication, the function should avoid a collision (a situation where two distinct messages have the same hash value), and it should be infeasible to find a message that hashes a given value. Actually the robustness of a hash function comes from the length of the message digest. Thus, the size of the message digest should be reasonably long to avoid any attempt to attack the hashing algorithm.

Although hash functions, in general, have many uses in computer programs, such as password encryption, in cryptography they are used to generate a small string (the message digest) that can represent securely a much larger string, such as a file or message. Since the hash functions are faster than the signing functions, it is much more efficient to compute a digital signature using a document's message digest than to use the arbitrarily large document itself. Additionally, a digest can be made public without revealing the contents of the document from which it is derived. This is important in digital time-stamping, where one can get a document without revealing its contents to the time-stamping service [Ref. 37: p. 47].

a. MD Series

MD stands for Message Digest. At present, MD2, MD4, and MD5 are widely used hash functions for cryptographic purposes, which were designed by Ron Rivest, one of the inventors of RSA public key algorithm [Ref. 37: p. 48].

MD2 takes a message equal to an arbitrary number of 8-bit bytes and produces a 128-bit message digest. Message inputs are padded with checksum, which is

a 16-byte quantity appended at the end of a message, then processed as a multiple of 16 bytes. By its 8-bit-oriented characteristics of processing, it is the slowest among the MD series. MD4 was designed to be 32-bit-word-oriented so that it can be computed faster on 32-bit CPUs than in a byte-oriented scheme. MD4 can handle messages with an arbitrary number of bits. To produce 128-bit digest, each of 512 bits is passed three times through a hash function [Ref. 38: p. 116].

MD5 is very similar to MD4, but is designed to be more conservative than MD4 in terms of being less concerned with speed and more concerned with security [Ref. 38: p. 120]. MD5 makes four passes over each 16-byte block. Fahn stated that MD5 is the most often recommended hash algorithm for digital signatures [Ref. 37: p. 48].

b. Secure Hash Standard (SHS)

The Secure Hash Standard (SHS) is a hash function proposed by NIST and adopted as a U.S. government standard, FIPS PUB 180, to check the integrity of data. It is designed for use with the DSS. SHS produces a 160-bit hash value from a variable size of input usually less than 2^{64} bits via five passes. The hash algorithm is similar to MD5 but, as it makes one more pass and produces longer hash value than MD5, it may be more secure than MD5.

5. Encryption in Networks

As mentioned before, encryption is a powerful tool to provide security services. In network applications, encryption can be applied either between two communicating hosts or between two applications. The former is link encryption, and the latter is end-to-end encryption. Usually, the location of the encryption scheme used in networks is well explained with the OSI reference model. In link encryption, the encryption occurs at layers 1 or 2 in the OSI model. In the end-to-end encryption occurs at the highest layers. Both methods have their pros and cons; thus, the selection decision depends on the situation or networks architecture, which requires encryption.

a. Link Encryption

In link encryption, data is encrypted just before it is placed on the physical communications link. Decryption occurs just as the communication enters the receiving computer. Encryption protects the message as it is in transit between two computers, but the message is in plaintext inside the hosts. Link encryption is invisible to the user or even the operating system. Thus, encryption is one service performed by a low-level network protocol layer as a hardware function, such as message routing or transmission error detection.

Link encryption is especially appropriate where the transmission line is the point of greatest vulnerability. If all hosts on a network are reasonably secure, but the communications medium is shared with other users or is not secure, link encryption is an easy control to use [Ref. 35: p. 376].

b. End-to-End Encryption

End-to-end encryption provides security from one end of a transmission to the other. The encryption is performed at a the highest levels of the OSI model (either the application layer or presentation layer), and can be applied by a hardware device between the user and host computer or software running on the host computer. The encryption can be done with software, so that it is easy to apply encryption selectively to one application or even to one message within a given application, although it requires human intervention [Ref. 35: p. 380]. As the message is only exposed by the user who has a proper device or software, it can pass any insecure node between two communications entity.

c. Link Encryption vs. End-to-End Encryption

In link encryption, the communicating hosts and other intermediate hosts must have the cryptographic facility to transmit a message, because both the message and

61

other headers (which contain information required to deliver the message to its destination) attached to a message are encrypted. Thus, all the hosts should be secure enough to prevent any message exposure. By contrast, in end-to-end encryption only communications hosts need the cryptographic facility since the intermediate hosts along a transmission path do not need to decrypt a message. Therefore, the message can be sent through any insecure networks although it can't prevent the passive attack, such as traffic analysis or network monitoring.

The number of required keys is another concern. With link encryption, the number of required keys depends on the network architecture; if very few hosts were directly connected to a single host, the number of keys would be fairly small, but if each node had a link to every other node, then the number of keys would be at most $n*(n-1)/2$ where n is the number of nodes. With end-to-end encryption, as the encryption is done with user, the number of keys is very large, which is $n*(n-1)/2$ for n users, not nodes. This number increases rapidly as the number of users increases. With the public key system, the number of key-pairs (public key and private key) is dramatically reduced to n for n users. However, as the public key encryption takes longer than the secret key and doesn't provide secrecy and authenticity at the same time, it may cause some overheads to solve these disadvantages.

In summary, link encryption is faster, easier for the user, and uses fewer keys. End-to-end encryption is more flexible, can be used selectively, involves the user, and can be customized to the application. If a user cannot trust the security provided by either link encryption or end-to-end encryption, both forms of encryption can be applied within a single network. If both encryptions are reasonably fast, this duplication of security will have little negative effect [Ref. 36: p. 380]. The applications of security service on the current commercial Internet well reflect the basic ideas of these approaches; the Secure HyperText Transfer Protocol (SHTTP) for end-to-end encryption, the Secure Sockets Layer (SSL) for link encryption, and Terisa Systems for both [Ref.

39]. The details of these approaches are described in the next section as "commercial Internet and transaction security."

C. APPLICATIONS OF DATA ENCRYPTION

1. Digital Signature

It is often useful to prove that a message was generated by a particular individual. In a networking environment, a message itself is usually not enough to provide the author's identity. Since business transactions using networks, such as EC/EDI, are increasing, the importance of proving the sender's identity and the legitimacy of a message is also increasing. In fact, the lack of secure authentication has been a major obstacle in achieving the promise that computers would replace paper [Ref. 37: p.18].

A digital signature is a protocol that produces the same effect as a real signature. It is a mark that only the sender can make, but others can easily recognize as belonging to the sender. Therefore, digital signatures should be strong against forgery and authentic. Pfleeger suggested two more properties that are desirable for digital transactions: not alterable and not reusable by others [Ref. 35: p. 134]. The efforts to develop a digital signature scheme were initiated with conventional cryptography and even without encryption techniques, but those approaches were not so successful. However, the use of the public key algorithm provides most of the properties required for a digital signature. At present, digital signature using public key cryptography with other integrity checking algorithms provides an effective way to convert the most essential paper-based documents to digital electronic media with authenticity and non-repudiation services.

a. Direct/Arbitrated Digital Signature

According to number of parties involved in the use of a digital signature, digital signatures can fall into two categories: direct digital signature and arbitrated digital signature. The direct digital signature involves only the communicating parties.

63

A digital signature may be formed by encrypting the entire message with the sender's private key, or by encrypting a hash value of the message with the sender's private key [Ref. 36: p. 186]. Confidentiality of a message can be provided by further encrypting the entire message plus signature with either the receiver's public key or a shared secret key. Direct digital signature is convenient and easy to use for internal communications or when the domain of communications is relatively small. The validity of this scheme depends on the security of the sender's private key, and on mutual trust.

Arbitrated digital signature involves an arbiter who plays a sensitive and crucial role to verify the signatures. With this scheme, every signed message from a sender goes first to an arbiter to check the origin and content, then to a receiver with additional information that states the message and signature are verified. Depending on the level of secrecy of the message contents, an arbiter may verify either a plain message with signature or an encrypted message with signature. In general, to use arbitrated digital signature, all communicating parties must have a great deal of trust that the arbitration mechanism is working properly [Ref. 36: p.187].

b. Choice of Digital Signature Techniques

To utilize the advantage of digital signature techniques, communicating parties (including arbiters if necessary) should use one technique to verify each other. At present, there are two distinguished techniques for digital signature: RSA algorithm and DSS. RSA public key algorithm is a de facto industry standard widely accepted by businesses. DSS is a U.S. Federal standard, which was published by NIST with the intention of royalty-free (no infringement on any patent right) algorithm for public use of digital signature. The procedures of digitally signing and verifying functions in these two techniques are briefly shown in Figure 7.

The comparison between these two digital signature techniques suggests that RSA algorithm has more advantages than DSS. First, RSA enables key-exchange and encryption of messages without using other mechanisms, when DSS requires other

mechanisms to provide confidentiality of a message. Actually, key-exchange and encryption may be done with a hardware device such as the Fortezza PC card. However, individuals and organizations that do not use that device still need to select a secure form of key-exchange or encryption mechanisms to achieve additional functions in DSS. Second, RSA is faster in signature verification, although DSS is faster in signature generation. But, as the actual necessity of digital signature is to verify message authenticity, faster signature verification is more widely considered for a characteristic of a good digital signature algorithm.
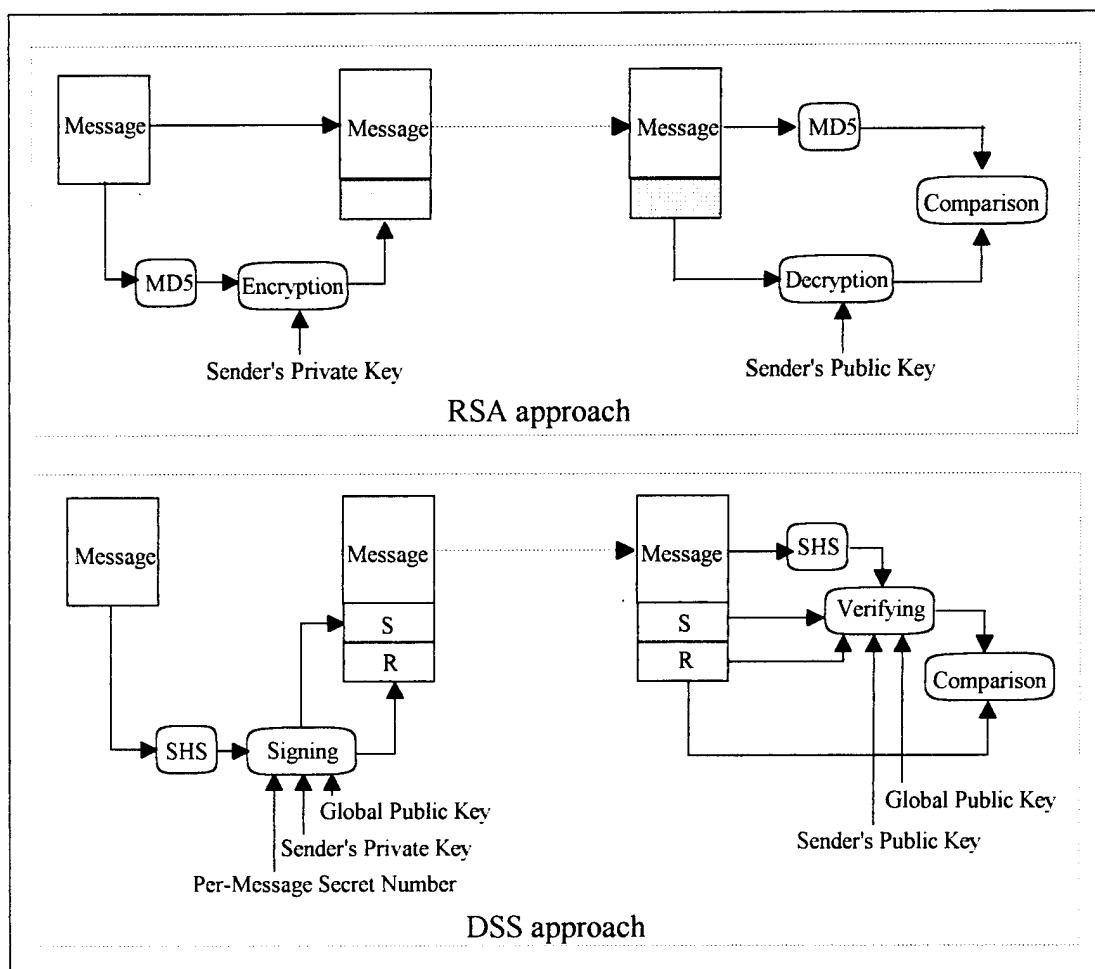
Figure 7. RSA/DSS Digital Signature [Mod. Ref. 36: p. 344]

The only advantage of DSS is its royalty-free option. However this advantage is only available for government use of DSS and for those vendors that deliver DSS products to the government [Ref. 40: p. 82]. Thus, commercial use of DSS should pay for the patent right of public key encryption, possessed by Public Key Partners (PKP). Although the publication of DSS as a federal standard represents an initiative of the government to enable EC/EDI, without the promise of free commercial use of DSS, it only gives limited incentives toward a ubiquitous digital signature scheme.

c. Digital Signature Certificate

In practice, a digital signature system requires a means for associating pairs of public and private keys with the corresponding users. Also, if digital signatures are to replace handwritten signatures, there must be a way to bind a user's identity and his/her digital signature so that it has the same legal status as handwritten signatures. In fact, digital signatures using public key algorithms, hash functions, and encryption are more immune to forgery, and have the potential to possess greater legal authority than handwritten signatures.

Since the validity of documents with digital signatures has never been challenged in court, their legal status is not yet well-defined. Through such challenges, the courts will issue rulings that collectively define which digital signature methods, key sizes, and security precautions are acceptable for a digital signature to be legally binding [Ref. 41]. At present, the legality of handwritten signatures is protected by several branches of law, such as the statute of Frauds, the Law of Acknowledgments, the Law of Agency, and the Uniform Commercial Code (UCC) [Ref. 41]. To achieve the same effect of legal protection related to signature, Pao suggested the use of an initial handwritten agreement defining the procedures and protocols for the utilization of digital signatures between senders and receivers [Ref. 45: p. 35].

To replace handwritten signatures with digital signatures, however, there should be an established government policy for handling signature certificates that validate

a user's electronic signature. To do this, this policy should define the relationship with previous policies, such as security structures in EDI (currently defined by ANSI X12.58 version 2) or public key certificate (ANSI X.509). Yet, as government initiation of DSS is different to industry's use of RSA, the settlement of this bi-directional approaches, and the cost of certificating digital signatures are current barriers against digital signature certificates.

2. Secure Mail Systems Using Data Encryption

In all distributed networking environments, electronic mail (e-mail) is the most heavily used network-based application. Actually, it is the only distributed application that is widely used across all architectures and vendor platforms [Ref. 36: p. 361]. The Internet provides a common basis for world-wide mail delivery service, directly or indirectly. With the explosively growing reliance on e-mail for every conceivable purpose, there grows a demand for secure e-mail systems. The requirements for a secure e-mail system include not only the services required by other network applications, but also mail-specific services, such as proof of submission, proof of delivery, or message flow confidentiality [Ref. 38: p. 333].

However, the Simple Mail Transfer Protocol (SMTP) supported by TCP/IP cannot satisfy all the demands of a secure e-mail system. At present, there are three standards related to secure e-mail services, which provide or specify those demands. This subsection briefly overviews security functions of those three approaches.

a. Privacy Enhanced Mail (PEM)

Privacy Enhanced Mail (PEM) was developed by the Internet community as a means of adding encryption, source authentication, and integrity protection to ordinary text messages [Ref. 38: p. 357]. The most common use of PEM is in conjunction with SMTP, but it can be used with any electronic mail scheme, including

67

X.400. To support this usage, PEM specifies dual address, one for SMTP, and another for X.400.

Actually, a message in PEM is composed of four types: (1) ordinary, unsecured data, (2) integrity-protected, unmodified data, (3) integrity-protected, encoded data, and (4) encoded, encrypted, integrity-protected data. These four types of sub-message can be encapsulated inside of one another. For encryption, PEM supports an RSA-based public key scheme (used for key interchange or key encryption) and two variants of DES (used for message encryption). To support public key technology, PEM defines a certification hierarchy based on the X.500 naming hierarchy (X.509 certificates and CDLs). For integrity protection and authentication, PEM supports RSA digital signature scheme with MD2 or MD5. Because PEM expects to handle ordinary text only, it has a encoding function to put messages into canonical form before encrypting them, or computing message integrity codes, so that the encrypted or signed form will not depend on the local formats of the system. [Ref. 38: p. 358 - 394]

b. Pretty Good Privacy (PGP)

In Pretty Good Privacy (PGP), mail message is only one variant of files, because PGP performs encryption and integrity protection based on files. Therefore, it is possible to process mail message as an ordinary file, then send it with other mail systems. However, for user convenience, a later version of PGP enables users to integrate PGP into their mail systems [Ref. 38: p. 400].

The cryptographic functions of PGP provides three types of message: authentication only, confidentiality only, and both. For authentication, PGP supports the RSA digital signature scheme with MD5. The difference between PEM and PGP in authentication function is that PGP delegates the management of public key certificates to the user, while PEM supports a rigid hierarchy of public key certificates in X.500. Thus, PGP provides three fields for doing this: the key legitimacy field, signature trust

68

field, and owner trust field [Ref. 36: p. 377]. For confidentiality, PGP supports IDEA for message encryption, and RSA for the IDEA session key encryption.

PGP canonicalizes only text files, and retains binary files as their own formats. An additional function of PGP is data compression. As a default, PGP compresses the message after applying the signature but before encryption [Ref. 36: p. 366]. This has the benefit of not only saving space for both e-mail transmission and for file storage, but also providing additional strength to the cryptographic algorithm.

c. X.400

X.400 is one of the CCITT's standards that describes the system model and Elements of Service of the Message Handling System (MHS) and Services. Rather than providing complete specifications of a system as PGP or PEM do, it only gives a framework for an implementation so that the implementor might decide specific types of system to fill "object identifier" that is remained as blank for interoperability. For this reason, X.400 does not specify any encryption algorithm (except RSA in X.509). The design of X.400 is reminiscent of post office mail, including features equivalent to certified mail and returned receipt mail. Interpersonal mail, defined in X.420, and EDI, defined in X.435, are certain the types of message that X.400 might carry [Ref. 38: p.413 - 415].

An X.400 message consists of two parts, envelope and content. The former is control information, and the latter consists of a header followed by a sequence of body parts. The security features of X.400 are provided by fields that are part of the envelope. All the security related fields in X.400 are optional. Parts of those security related fields within the envelope are per-message security fields that define key certificates, message confidentiality, origin authentication, and other secure message handling functions. They also define six levels of message security classification from unmarked to top secret. However, the details of dealing with these different class of message are not specified. One of the security fields mentioned in X.420 is encrypted

body parts. Yet, the parameters of such a body part and the encryption technique are not specified, either. [Ref. 38: p. 417 - 424]

As X.400 security has not been really deployed, Kaufman et al. suggested that a perfectly reasonable method of obtaining mail security with X.400 is to use the PEM body part, and use PEM for encryption, integrity protection, and source authentication [Ref. 38: p. 419] . This approach is simple to implement but PEM is only for text and there might be an extreme overhead when encoding multi-media (such as video, audio, or facsimile) messages into text format.

3. Commercial Internet and Transaction Security

While the proliferation of the Internet enables easy access to information distributed across thousands of computers, businesses are also tring to find a way to convert their business processes from paper transactions to digital, on-line transactions via Electronic Commerce/Electronic Data Interchange (EC/EDI). But security risks are still the major concern threatening their actual movement toward EC/EDI. Many transactions require the ability to protect confidential information, authenticate the source of communications, ensure the integrity of message content, and verify the transmission and receipt of a message.

The term "transaction security" refers to the networks services that satisfy all these requirements. At present, two different approaches are initiated for the transaction security. These are Secure HyperText Transfer Protocol (SHTTP) and Secure Sockets Layer (SSL) Protocol. SHTTP marks individual documents as private or signed at the application layer of OSI model, while SSL mandates the channel of communication between two parties as private and authenticated by encrypting the documents at the top of the transport layer. Since these approaches were initiated separately with different perspectives and still compete with each other for the final approval as a common security standard, there may be a non-interoperability problem between SHTTP and SSL. Rather

than selecting one approach, the Terisa system [Ref. 39] suggested a new approach adopting those two approach altogether.

a. Secure HTTP (SHTTP)

HyperText Transfer Protocol (HTTP) is the internal communications protocol of the World-Wide Web. Secure HTTP (SHTTP) is security enhanced version of HTTP that was developed by Enterprise Integrated Technologies (EIT) Inc., and is now available to the Internet community as a non-proprietary specification [Ref. 40]. It provides secure communication mechanisms between an HTTP client-server pair in order to enable spontaneous commercial transactions for a wide range of applications. The protocol emphasizes maximum flexibility in the choice of key management mechanisms, security policies and cryptographic algorithms by supporting option negotiation[6] between parties for each transaction.

SHTTP is one example of end-to-end encryption. Security functions are located at the highest level of the OSI model, the application layer. The message protection may be provided by signature, authentication, and encryption. For digital signature, it supports both RSA and DSA schemes. For message integrity and user authenticity, it supports the Message Authentication Code (MAC) via manual arrangement or Kerberos. For encryption, it supports symmetric key algorithms, such as DES or RC2, with various key-exchange mechanisms, including the public key scheme. The major cryptographic message format standards supported by SHTTP are PKCS-7, PEM, and PGP, although the format standards are not limited to those three standards [Ref. 42]. After all, the message block consists mainly of four portions: the main SHTTP header, encapsulated non-negotiation header, encapsulated negotiation header, and privacy enhanced original message.

---

[6] Negotiation is a method to express the requirements and preferences regarding what cryptographic enhancements will be permitted/required between two communicating parties [Ref. 42: p. 11].

71

b. Secure Sockets Layer (SSL) Protocol

The Secure Sockets Layer (SSL) Protocol, developed by Netscape Communications Corp., is a security-enhanced abstraction of sockets that provides transaction security at the link or transport level [Ref. 39]. Thus, it allows client-server applications to communicate in a way that precludes eavesdropping. With SSL, security properties are attached to the link or channel of communication between two parties, not the documents themselves.

To provide communications channel security, SSL Protocol uses secret key cryptography for data encryption (e.g., DES or RC4[7]), public key cryptography for authentication (e.g., RSA), hash functions for data integrity (e.g., MD2 or MD5). Actually, SSL Protocol is composed of two protocols: the SSL Record Protocol and the SSL Handshake Protocol. The former is used for encapsulation of all transmitted and received data, including the SSL Handshake Protocol, in records. The record is a certain unit of length composed of a header portion and data portion. SSL Handshake Protocol is a series of phases used to establish security parameters negotiated by client and server application [Ref. 43]. The main advantage of SSL Protocol is that it is application protocol independent; thus, any higher-level application protocol can layer on top of the SSL protocol transparently. Currently, Netscape Communications Corp. introduced another protocol (Secure Courier), which is based on SSL, for transmitting financial data over the commercial Internet based on SSL.

c. Summary

In summary, SHTTP has the capability to provide comprehensive security in a flexible manner, but the service is limited to the Web-specific applications. SSL is a more generic security protocol, but it can support any applications using TCP/IP.

---

[7] The export version of SSL uses 40-bit RC4, where as U.S. version uses 128-bit RC4. The 40-bit RC4 was broken by brute force attack in August 1995, thus, there is a bit wonder about the security feature of export version of SSL.

Although these two emerging approaches utilize a variety of industrial standards and protocols, such as HTTP, TCP/IP and RSA public key cryptography, they are unable to communicate with each other. To allow the businesses to take advantage of the strength of both protocols, the Terisa Systems, a joint venture company by Enterprise Integration Technologies and RSA Data Security Inc., provides the unified approach by adopting those two different protocols at one package. However, it may be a piggybacking approach for transaction security and maybe required only by a big organization that actually needs a strong interoperability between SHTTP and SSL.

The decision to select the most beneficial protocol for EC/EDI data transaction among these three approaches is not easy. To select a proper tool, one should consider not only requirements for data security and current communications architecture, but also the direction of international trends for security standards.

D. FIREWALL/SECURITY GATEWAYS

1. Introduction

A firewall is any one of several ways of protecting an internal network from other untrusted networks by filtering packets according to various criteria, usually based on the organization's network security policy. Security Gateway is just another name for a firewall. The main purpose of a firewall is to prevent unauthorized users from accessing computing resources on a private network, and often to prevent unnoticed and unauthorized export of proprietary information. In the latter case, the export of information is usually not considered important, because the internal user might have more convenient ways, such as floppy diskettes or magnetic tapes, to export those proprietary information rather than using networks.

The necessity of a firewall comes from two reasons: a growing use of global untrusted networks, such as the Internet, and a lack of security features in the design of organization's networks and network operating systems. The Actual mechanisms of a

firewall are mainly divided into two categories: blocking traffic and permitting traffic. In configuring a firewall, these mechanisms represent the organizational policy over existing or anticipated levels of threat. If security is more important than anything else, the firewall would be designed to block everything except minimum network traffic that comes from known, trusted networks of well known applications forms such as e-mail.

The location of a firewall should be carefully analyzed so that it examines and evaluates all traffic passing through it, without exception. If there are more than one connection points to outside networks, several firewalls will be required, or the inside network may be modified to permit only one connection point to the outside. However, to avoid being a bottleneck of networking, the firewall should have enough capacity to control traffic. The component of a firewall system can be a router, a personal computer, a host computer, or a combination of these.

2. Firewall Components

a. Packet Filter

Packet filters can provide a cheap and useful level of gateway security. It is the simplest form of a firewall, and it selectively discards packets based on configuration rules. IP packet filtering is usually done with a router designed for filtering packets as they pass between the router's interfaces. A packet filtering router usually can filter IP packets based on four fields: source IP address, destination IP address, TCP/UDP source port, and TCP/UDP destination port [Ref. 44: p. 24]. A specially designed host computer can also perform packet filtering with additional functions of traffic monitoring and auditing. Filtering can be used in a variety of way to block connections from or to specific hosts or networks, and to block connections to specific ports, depending on the capability of filtering software.

Packet filtering has a number of weaknesses. IP address based filtering does not give any protection against address spoofing attack. The filtering rules are

complex to specify and, usually, no testing facility exists for verifying the correctness of the rules. Some network services (such as RPC service using UDP) randomly assign port numbers so that it is hard to block unfixed port numbers with a fixed rule set of packet filters. Undetected errors in filtering software and holes in rule set may exist until a break-in has occurred[8]. As packet filters may permit direct communication between multiple hosts on the private network, and multiple hosts on the outside networks, they do not provide users with confidence in their correctness and hence their safety. However, packet filters are a useful tool on which many advanced gateway designs rely [Ref. 45: p. 77] .

b. Application-Level Gateway

An application-level gateway uses a special-purpose code for each desired network application, rather than using a general-purpose mechanism to allow many different kinds of traffic to flow. It is far more secure than any of the alternatives. [Ref. 45: p. 75]. Such a special-purpose code is referred to as a proxy service, and handles packets between Application Layer and Transport Layer of the TCP/IP protocol stack.

The proxy service intercepts the service request packets, which are passed through a routing device, and go up through each layer of the TCP/IP protocol suite until the Application Layer, then checks its table, and denies or grants access to the service, based on the source's Internet address and the service being requested. If the service is denied, the packet is dropped, the event logged, and nothing further is done. If the service is granted, the event is logged, and the packets are passed on to the server, which provides the requested application [Ref. 46: p. 23 - 24].

An application-level gateway may have several proxy services designed for FTP, SMTP, TELNET, DNS, or NFS. Compared to pure packet filters, the main advantage of application-level gateways is the reduced work of packet filtering. As each

---

[8] Cheswick and Bellovin presented two examples for this: CERT Advisory CA-92:20 and CA-93:07 [Ref. 46: p.75].

proxy service can deal with one type of application-specific packets, the filtering rule set is less complex, and will not affect other resources in the private network. Also, some proxy services can provide a protocol filtering service to avoid harmful requests of service (such as the "put" command in FTP connections) [Ref. 44: p. 30].

The principle disadvantage of the application-level gateway is the need for a specialized user program or variant user interface for most services provided [Ref. 45: p. 76]. Thus, in general, the most important or most popular services can be supported in conjunction with the other gateway designs.

c. Circuit-Level Gateway

A circuit-level gateway relays TCP connections but does no extra processing or filtering of the protocol. It is sometimes included under the category of the application-level gateway [Ref. 45: p. 31]. When the connection between the source and destination is established, the firewall simply passes bytes between the systems as a wire does. In general, it is designed to allow open connection to a trusted host located outside of the private network, with specially assigned ports.

3. Applications of Firewall Design

a. Packet Filtering Firewall

The packet filtering firewall that uses screening routers is the most common and easiest to employ for small, uncomplicated sites, since it permits fairly free access to WAN from any point within the private network. However, as mentioned in the previous subsection, there are many problems in a pure packet filtering router. Thus, the firewall design using only a screening router is not enough to provide required security for the private network.

b. Dual-Homed Gateway Firewall

The dual-homed gateway consists of a host system (sometimes called a bastion host) with two network interfaces, and with the host's IP forwarding capability disabled. Unlike the packet filtering firewall, the dual-homed gateway is a complete block to IP traffic between WAN and the protected private network. Both the private network hosts and outside hosts can talk only to the gateway. The connection between the private network and WAN is controlled by proxy services residing on the gateway. Thus, the gateway denies all services unless they are specifically permitted by proxy services. The disadvantage of the dual-homed gateway firewall is its inflexibility to other services that are not provided by proxy services [Ref. 45: p. 36]. The other security concern of this option is the strength of gateway. Since the gateway provides all protection for the private network, any weakness in the gateway may compromise the security of the entire private network.

c. Screened Host Firewall

The screened host firewall is a more flexible firewall than the dual-homed gateway firewall, however the flexibility is achieved with some cost to security. It combines a packet filtering router with an application gateway that has only one interface to either the private network or WAN side. In this configuration, certain trusted services may pass through the gateway if the gateway does not have the required proxy service; hence, the firewall is more flexible but less secure than the dual-homed gateway option. The actual decision regarding construction of this firewall could reflect a mixture of the two design policies, the proportions of which depend on how many and what types of services are routed directly to the private network [Ref. 45: p. 36 - 38].

77

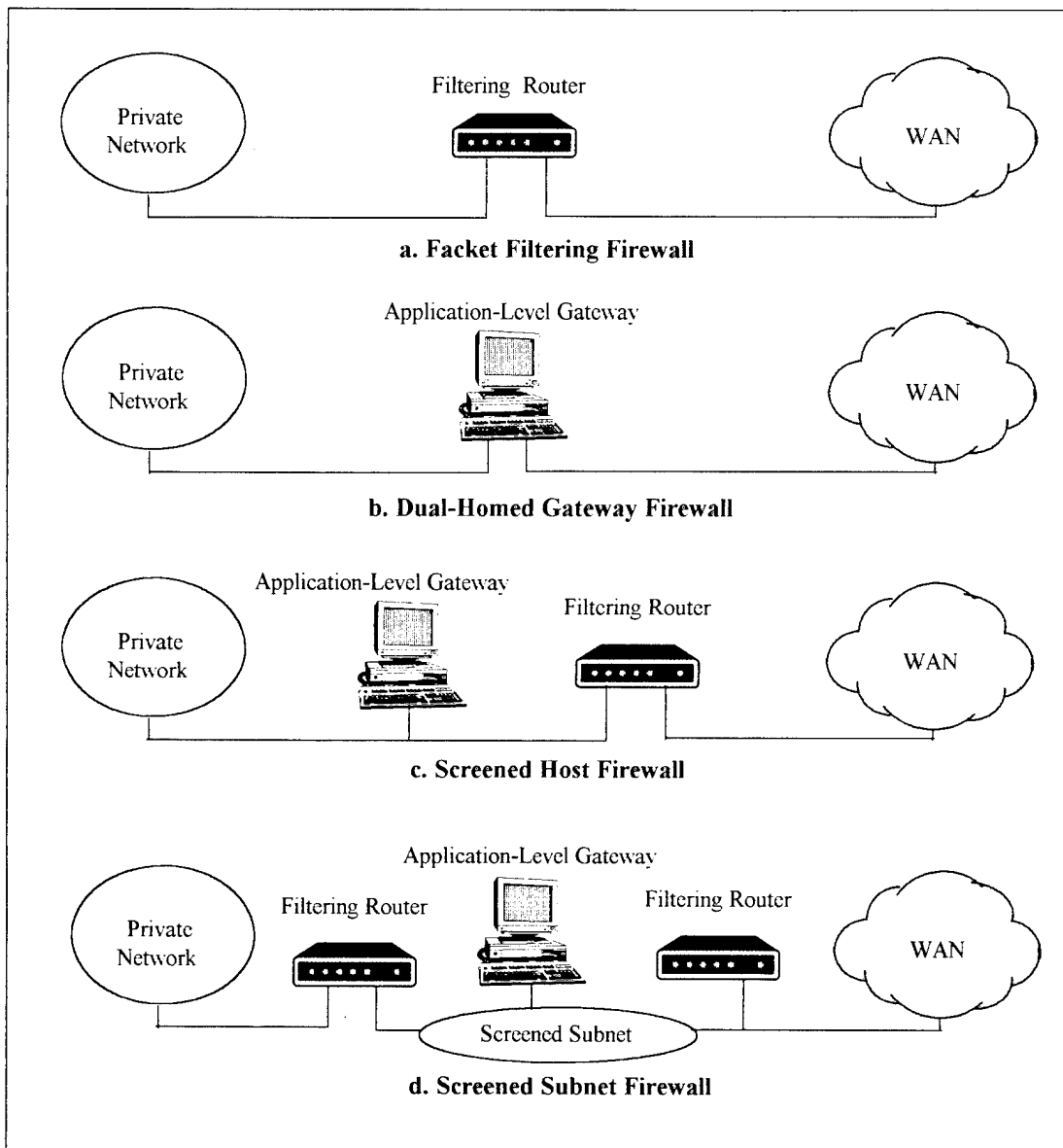**Figure 8. Applications of Firewall Design**

d. Screened Subnet Firewall

The screened subnet firewall consists of two routers and an application-level gateway. It is a variation of the dual-homed gateway and screened host firewalls. In this configuration, there are three portions of networks: the private network, screened subnet (sometimes referred to as "DMZ"), and WAN. On the screened subnet,

the application-level gateway and other network service hosts (such as the FTP server and e-mail server) can be located more securely than other firewall options without affecting the security of the private network. The outer router restricts access from outside to specific systems on the screened subnet. The inner router passes traffic to and from systems on the screened subnet. These two routers are used to direct traffic to specific systems, eliminating the need for the gateway to be dual-homed. Consequently, this firewall configuration may be more appropriate for sites with large amounts of traffic, or sites that need very high-speed traffic. Also, each component of the firewall needs to implement only a specific task; thus, the systems are less complex to configure. However, in terms of security, it is less desirable than the dual-homed gateway because it might be possible to allow certain trusted services from outside to private network [Ref. 45: p.40].

4. Trusted Guard Gateway (TGG)

In the CALS telecommunications security plan, Doby reported the necessity of the Trusted Guard Gateway (TGG), which was intended to provide security and interoperability among DDN segments (ARPANET, MILNET, DISNET) [Ref. 2: p. 22 - 24]. For security, the role of TGG is to provide limited but secure communications between the communities whether operating at different levels of trust or at different levels of security. Figure 9 shows three different types of TGG: a MILNET/DISNET TGG, an ARPANET/MILNET TGG, and a closed-community/open-community TGG.

The MILNET/DISNET TGG is a gateway that supports unclassified communications between two different security levels of network. It requires more secure and intelligent capability than general purpose firewalls, since it involves security classification upgrading or downgrading when the information is classified. Also, it requires an end-to-end encryption device, such as BLACKER, to avoid any possible classified information exposure [Ref. 2: p. 2].

79

Sensitive but unclassified
Trusted Users (MILNET)

Commercial
Networks

Closed
Community

PSN — TGG

Open
Community

TGG   TGG

Classified Users
(DISNET)

Unclassified
and
Untrusted Users
(ARPANET)

Closed
Community

TGG — PSN

Open
Community
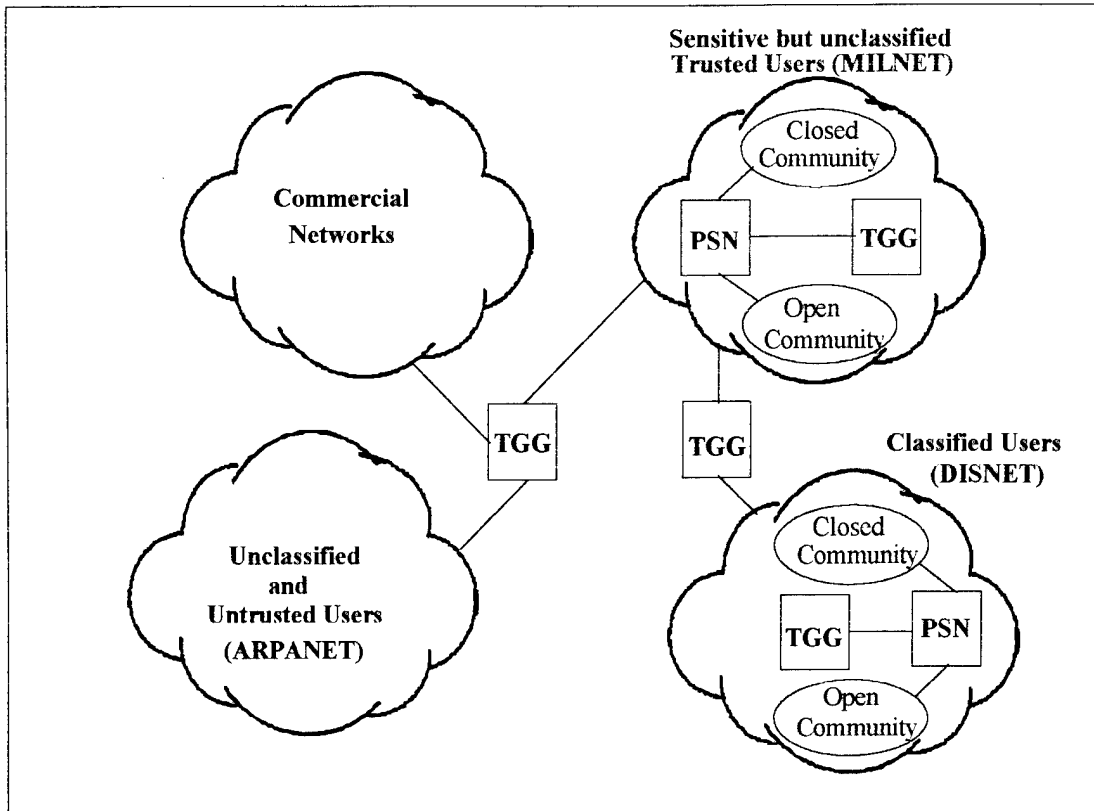
Figure 9. Trusted Guard Gateways in DDN [Ref. 2: p. 23]

The ARPANET/MILNET TGG was primarily intended for e-mail transfer and limits other traffic between two networks that were separated from DDN in 1983. It can be considered as a firewall using an application-level gateway that provides limited network services. Although the information may not classified in MILNET or Commercial networks, the design criteria of the gateway should represent the security policy of related networks to provide required protection for sensitive information.

The third type of TGG was intended to limit communications between open and closed communities which were included in a same level of network. The reason of this consideration came from the lack of security certification of host computers, which was intended to the C2 level or better. The non-certified hosts would be grouped as the closed community and only have limited access to other side of community through TGG.

The three types of TGG shows a model of actual firewall design specifically required to the military subscribing host computers. As CALS communications require interconnection between industry networks and military networks, the firewall design should be considered one of the important resources to provide proper protection against any possible information exposure.

5. Firewall and Security Policy

Firewalls are a powerful tool for network security. However, it should be considered that firewalls also have their limitation. Though firewalls are very strong defense against attacks at a low level of the protocol stack, in contrast, firewalls provide almost no protection against problems with higher level protocols [Ref. 45: p. 82]. Firewalls cannot protect against attacks that do not go through the firewall. As attacks against private networks always seek the most vulnerable point, any open connection which is not protected by firewalls makes the elaborate efforts of constructing firewalls all for naught. Firewalls cannot protect against a data-driven attack -- attacks in which something is mailed or copied to an internal host where it is then executed[9]. Even though known contexts of data-driven attacks are scanned during it passes through the firewall, still there is possibility of unknown types of attack.

Cheswick described the firewall as, at best, a convenient single place to apply a corrective filter [Ref. 45: p. 83]. However, the realistic firewall policies that reflect the level of security in the entire network can provide adequate protection for the non-classified information. Even more, combined with encryption tool, it might be applicable high level secure data delivery.

The users act very important role in the firewall configuration. Misuse or flouting of the security policy can easily bring security holes on the entire networks. It is obvious that firewall cannot replace security-consciousness of users on the private network. Thus,

---

[9] The Internet Worm is one of the notorious example of this type of attack.

the users on the network should be continuously aware of the firewall policies to achieve overall security of their systems.

V. SECURITY MANAGEMENT OF CALS TELECOMMUNICATIONS

A. CALS SECURITY REQUIREMENT

When CALS automates and integrates digital, processable information using a shared database, it should be implemented with a proper means to protect this shared data environment from unauthorized access, use, or alteration throughout the life-cycle of a weapon system. To protect and assure the integrity of CALS data, DoD presented six interrelated security disciplines based on DoDD 5200.28, Security Requirements for Automated Information systems [Ref. 13: p.204]:

- Communications Security (COMSEC): The protection resulting from the application of transmission security, crypto security and emission security measures to telecommunications, and from the application of physical security measures to COMSEC information.

- Computer Security (COMPUSEC): The totality of security safeguards needed to provide an acceptable level of protection for Automated Data Processing (ADP) systems and the sensitive data processed.

- Physical Security: The physical measures that are designed to prevent unauthorized access to equipment, facilities, material, and documents, and to safeguard against espionage, sabotage, damage, and theft.

- Personal Security: The measures whereby the trustworthiness and suitability of personnel are verified for positions of trust based on information regarding their loyalty, character, emotional stability, and reliability.

- Information Security (INFOSEC): The measures and administrative procedures for identifying, controlling, and protecting against unauthorized disclosure of classified information or sensitive unclassified information.

- Operations Security (OPSEC): The protection of operations resulting from the identification and subsequent elimination or control of intelligence indicators susceptible to compromise.

To satisfy all of these security requirements is not an easy task. It may add further costs to the CALS implementation. However, it is very important to assure the data protection and integrity for the future of fully integrated information systems. Were it not a proper protection mechanism, the potential participants of the integrated information system might fear the word "integration" or "data sharing." Thus, the cooperation between government and industry for establishing adequate security protection to an integrated information system should exist, in addition to the integration efforts.

This chapter will analyze such a mechanism to satisfy security requirements for CALS telecommunications. Security is only as good as its weakest point. Therefore, the security management of CALS telecommunications should concentrate on identifying the weakest point of overall security, and on providing an adequate protection mechanism for that point.

B. SECURITY POLICIES AND STANDARDS RELEVANT TO CALS

1. Overview

The Automated Interchange of Technical Information (MIL-STD-1840) and CITIS (MIL-STD-974) are a good starting point to assess the requirements for the secure CALS telecommunications plan. Usually, MIL-STD-1840 and CITIS are considered mutually exclusive concepts dealing with delivery methods of CALS data in a physical form or an electronic one. In fact, those two standards are complementary rather than mutually exclusive. Because MIL-STD-1840 was designed to support a digital data delivery, the standardized header records specified in the standard are very important for CITIS's function of data configuration management, including data dictionary and data directory services. Security features in these two standards are shown below:

a. MIL-STD-1840B

The current version of MIL-STD-1840 defines the formats, standardized header records, and the contents of the files used for the exchange of data as well as requirements for labeling, protection, packaging, and the making of media during shipment. According to MIL-STD-1840B [Ref. 47], each transfer package may consist of one or more transfer sets, which include multiple transfer units. Each transfer unit has a unit declaration file, which has 17 fixed length records of 128 bytes each, and several unit data files. Two security related records in the unit declaration file are:

- Title Security Label (ttlcls): A character string stating the security/sensitivity level or other restrictions on the title of the document.

- Document Sensitivity Label (doccls): A character string stating the highest security/sensitivity level or other restrictions on any file in the transfer unit.

A unit data file has fixed-length head records describing all the characteristics of a data file. It is fixed length, but the actual length may depend on the data file type specified by a contract. Among various head records, there are two security related records:

- Source System Document Identifier (srcdocid): A character string used by the source system to uniquely identify the document to which this file belongs, comprises, or applies. Position 57, data rights, and position 61, security classification, are two important elements.

- Data File Security Level (doccls): Character string stating the security/sensitivity level or other restrictions on the data file.

As many of the standards and specifications required or referenced by MIL-STD-1840B are evolving significantly due to rapidly advancing technologies, these will have to be implemented further in a future revision of this standard [Ref. 8: p. 12-9]. The candidates of these standards and specifications are IETM, EC/EDI, PDES,

telecommunication standards (X.400, X.435, X.500), and methods of compression and encryption.

b. Contractor Integrated Technical Information Service (CITIS)

The CITIS (MIL-STD-974) was developed to provide the government with electronic transfer of, and access to contractor-maintained data and Government Furnished Information (GFI), as specified by the contract. The capability of electronic transmission of data using CITIS is not limited to the government and its contractors. It also can be used for electronic data transmission among business partners in usual business contracts. The present version of CITIS defines the role of CITIS as information service, data configuration management, CITIS security, data item index, and other functions [Ref. 18: p. 7].

There are two functions in CITIS: core and tailorable. The core functions deal with basic functional requirements[10] required for on-line delivery of data instances. Tailorable CITIS functions are more complicated than core functions, because those functions deal with a directory or dictionary of data items to support application softwares, packages of user selected data items, or queries. Tailorable functions require a reasonable telecommunications capacity to enable on-line data transfer between the government site and the contractor; thus, these functions may be limited until the Defense Information Infrastructure is modernized.

As CITIS uses networks connecting CITIS sites, all the security issues mentioned in Chapter IV are inherent in CITIS. Also, as information provided by CITIS may include a combination of differently classified data, each data item in each different level of classification should be properly marked for proper access control. Examples of parameters that define the access rule set include: information type; information access strategy; data status level; type of access; classification and sensitive data limitations;

---

[10] The functional requirements include acknowledgment of delivery of data instances, approval of data instances and logging, comment on data, receive, search, store, and view function.

distribution limitations; maximum allowable number of unsuccessful or improper access attempts; and the authorized user's security clearance, organization, location, CITIS read/write authorizations, and access profile [Ref. 18: p. 14].

CITIS can use data formats specified in MIL-STD-1840 as a data exchange standard. However, both security reasons and the requirements to support application softwares (which will be used in the future CALS environment) suggest that the header format of data elements specified by MIL-STD-1840 may not be sufficient for CITIS's use. Since MIL-STD-1840B specifies off-line delivery methods of CALS data as a package, there may be some redundancy of data when users store separately delivered packages in their own databases. As CITIS promises delivery of data in terms of data elements, there should be more specific information in the head of each data element related to the data dictionary/directory service. Thus, to adapt CALS as a national strategy to develop information technology, earlier consideration of security-specific fields and transmission-specific fields in data element headers will reduce further revising efforts.

2. Trusted Computer System Evaluation Criteria (TCSEC)

Trusted Computer System Evaluation Criteria (TCSEC) is one of the most widely acclaimed documents for Trusted Computing Base (TCB). Published by DoD in 1983 and revised in 1985, TCSEC provides authoritative guidance, measurement, and acquisition criteria for evaluating the security features of computer systems. For guidance, it provides a standard to manufacturers as to what security features to build into their new and planned commercial products in order to satisfy trust requirements for sensitive applications. For measurement, it provides users with a metric to evaluate the degree of trust that can be placed in computer systems for the secure processing of classified and other sensitive information. For acquisition, it provides a basis for specifying security requirements in acquisition specifications [Ref. 48: p. 2].

a. Fundamental Computer Security Requirements

TCSEC defines secure systems as those systems that control, through use of specific security features, access to information such that only properly authorized individuals, or processes operating on their behalf, will have access to read, write, create, or delete information. From this definition, TCSEC derives six fundamental requirements:

- Security Policy: Given identified subjects and objects[11], there must be a set of rules that are used by the system to determine whether a given subject can be permitted access to a specific object. This policy further specifies mandatory security control[12] and discretionary security control[13].

- Marking: Access control labels must be associated with an object. This capacity, together with mandatory security policy, ensures that clearances associated with users and objects accurately reflect the security levels of these subjects and objects.

- Identification: Each access to information must be mediated, based on who is accessing the information, and what classes of information they are authorized to deal with.

---

[11] An object is a passive entity that contains or receives information, such as records, files, directories, and programs. A subject is an active entity, generally in the form of a person, process, or device that causes information to flow among objects, or changes the system state [Ref. 48: p. 116].

[12] Mandatory security control enforces a system by a set of rules for controlling access based directly on a comparison of the individual's clearance or authorization for the information and the classification or sensitivity designation of the information, and indirectly on considerations of physical and other environmental factors of control.

[13] The term discretionary security control refers to a system's ability to control information on an individual basis. In the discretionary security enforced system, even though an individual has formal clearance for access to specific information, each individual's access must be based on a demonstrated "need-to-know" [Ref. 48: p. 74 -75].

- Accountability: The occurrence of security-relevant events in an audit log must be kept and protected selectively so that actions affecting security can be traced to the responsible party.

- Assurance: The computer system must contain hardware/software mechanisms that can be independently evaluated to provide sufficient assurance that the system enforces the requirements shown above.

- Continuous Protection: The requirements must be continuously protected against tampering and/or unauthorized changes.

b. Divisions of Security Protection

TCSEC specifies four hierarchical divisions of security protection criteria: D, C, B, and A. Division D is reserved for systems that have been evaluated but fail to meet those security requirements. Division C has two classes: C1 and C2, which require discretionary access control protection. Division B has three classes: B1, B2, and B3, which require support for sensitive labels. Division A has only one class, A1, which requires additional assurance through formal verification methods. The classes and their security requirements are shown in Table 7.

- C1 (Discretionary Security Protection): This class nominally satisfies the discretionary security requirements by providing separation of users and data. It incorporates some form of credible controls capable of enforcing access limitations on an individual basis. The class C1 environment is expected to be one of cooperating users processing data at the same level of sensitivity.

- C2 (Controlled Access Protection): This class enforces a more finely grained discretionary access control than C1 class, making users individually accountable for their actions through login procedures, auditing of security- relevant events, and resource isolation.

- B1 (Labeled Security Protection): In addition to C2 requirements, this class enforces the preparation of informal statements of security policy models, data labeling, and mandatory access control over named subjects and objects.

Table 7. TCSEC Summary Chart

Security Requirements		D	C1	C2	B1	B2	B3	A
								Classes
Security Policy	Discretionary Access Control							
	Object Reuse							
	Labels							
	Label Integrity							
	Exportation of Labeled Information							
	Exportation to Multi-Level Devices							
	Exportation to Single-Level Devices							
	Labeling Human-Readable Output							
	Mandatory Access Control							
	Subject Sensitive Labels							
	Device Labels							
Accountability	Identification and Authentication							
	Audit							
	Trusted Path							
Assurance	System Architecture							
	System Integrity							
	Security Testing							
	Design Specification and Verification							
	Covert Channel Analysis							
	Trusted Facility Management							
	Configuration Management							
	Trusted Recovery							
	Trusted Distribution							
Documentation	Security Features User's Guide							
	Trusted Facility Manual							
	Test Documentation							
	Design Documentation							

Legend:
New or enhanced requirements: ☐
No additional requirements: ☐
No requirements: ▩

- B2 (Structured Protection): This class enforces the use of formal security policy models that require discretionary and mandatory access control enforcement used in B1 class to be extended to all subjects and objects in the Automated Data Processing (ADP) system. Compared to B1 class, it has many more security features to assure the security of systems.

- B3 (Security Domain): This class must satisfy the reference monitor requirements that mediate all accesses of subjects to objects; it must be tamper-proof and small enough to be subjected to analysis and test.

- A1 (Verified Design): This class is functionally equivalent to B3. The distinguishing feature of this class is the analysis derived from formal design specification and verification techniques, and the resulting high degree of assurance that the TCB is correctly implemented.

c. Security Modes of Operation

When the systems evaluated by TCSEC are used in an actual operation, the security modes can be defined by a manner in which the access requirements for user clearance level and need-to-know[14] are implemented in the Automated Information System (AIS). Security modes are authorized variations in security environments and methods of operating trusted systems that handle classified information [Ref. 50: p. 8-2-1]. To provide adequate protection of classified information while allowing users to access proper information, these modes may be tailored by the organization. Current security operating modes defined by NCSC are shown below [Ref. 51: p. 9 - 10]:

- Dedicated Security Mode: The dedicated security mode is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time.

- System High Mode: The system high mode is defined by software/hardware trusted to provide only need-to-know protection

---

[14] Need-to-know is defined as a determination made by a possessor of classified information that a prospective recipient has a requirement for access to, knowledge of, or possession of the classified information in order to accomplish lawful and authorized government purposes. [Ref. 50: p. I-9]

between users. In this mode, the entire system must operate with security measures commensurate with the highest classification and sensitivity of the information being processed and/or stored. All system users in this environment must possess clearances and authorizations for all information contained in the system. All system output must be clearly marked with the highest classification until the information has been reviewed manually by an authorized individual to ensure appropriate classifications.

- Partitioned Security Mode: In this mode of operation, all users have clearance but not necessarily formal access approval and need-to-know for all information contained in the system. This means that some users may not have need-to-know and formal access approval for all data processed by the AIS system.

- Compartmented Security Mode: The compartmented security mode is a mode of operation in which each user has a valid clearance for the most restricted intelligence information processed in the AIS. Each user also has formal access approval, a valid need-to-know, and a signed nondisclosure agreement for that intelligence information to which the user is to have access.

- Multi-Level Security Mode: In this mode, not all users have a clearance or formal access approval for all data handled by the AIS. The components used in this mode must have the technical capability to control access to information based on need-to-know, formal access approval, and sensitivity level of the data in the system.

3. Trusted Network Interpretation (TNI) of the TCSEC

As a network involves many systems that often have various security levels and modes, there is a necessity to control the network either component by component or as a entire system. The Trusted Network Interpretation (TNI) and Trusted Network Interpretation Environments Guideline (TNIEG) are an effort of NCSC to interpret the TCSEC for networks. The TNI contains all of the criteria in the TCSEC, and adds interpretation and rationale to applying trust technology to network systems. It focuses on policy and assurance features necessary to achieve a certain level of security

accreditation. The TNIEG provides guidance for the use of the TNI by identifying the minimum security protection required in different environments [Ref. 52: p. 1].

a. Two Network Views

The TNI distinguishes two alternative views for accreditation and evaluation purposes: as a single unified system or as an interconnection of two or more independently accredited automated information systems.

In the first perspective, a network is regarded as an instance of a single trusted system. A more accurate view is when some of its AIS subsystems are so specialized or dependent on other subsystems of the network for security support that individual accreditation of such subsystems is not possible or meaningful with respect to secure network operation. In order to be accredited, the unified system should have a coherent network architecture and design, and it should be developed with an attention to security requirements, mechanism, and assurances commensurate with the range of sensitivity of information for which it is to be accredited [Ref. 52: p. 10]. Examples of "single trusted systems" include packet-switched networks, end-to-end encryption systems, application level networks, and local area networks [Ref. 53: p. xv].

Interconnected, accredited AIS consists of multiple systems that have been independently rated and accredited to process sensitive information at a single level, or over a range of levels. Because of the complex structure of a network requiring accreditation rules for connection components, it may not be practical to evaluate such a network using this interpretation, or to assign it a trusted system rating [Ref. 53: p. xiii]. However, when a unified system view is not appropriate to accredit a certain network, this view would be used with careful consideration. Appendix C of the TNI explains the rules and situations required to evaluate a network with this view.

b. Network Security Architecture and Design (NSAD)

The Network Security Architecture and Design (NSAD) shows how the Network Trusted Computing Base (NTCB) is partitioned, and how the trusted system requirements are met. NSAD results from a series of tradeoffs among cost, effectiveness, technical risk, mission requirements, and risk management of a network. While the architecture of the NSAD may be somewhat abstract, the design should be quite concrete by mapping the selected security services to system functional elements. The NSAD for a network must address the applicable security-relevant policies, and may incorporate the NSADs of its constituent components or subsystems [Ref. 52: p. 15].

c. Security Requirements for Network

The TNI divides security requirements of trusted networks into two parts: minimum security requirements, which interpret the TCSEC for networks; and qualitative evaluation of security services in terms of functionality, strength of mechanism, and assurance. Determining the minimum security requirements for a network is nearly the same as for a stand-alone system. Additional factors such as communications security, distance between devices, number of subsystems, and encryption are considered to determine the minimum security requirement. Part two, qualitative evaluation of security services are concerned with functionality, strength of mechanism, and assurance of those services that are more network-specific (e.g., communications integrity, non-repudiation, and network management, etc.) [Ref. 53: p. 163, 177].

4. System Security Engineering Program Management Requirements (MIL-STD-1785)

The System Security Engineering (SSE) program defines the role of security throughout the life-cycle of the major development and/or upgrade program, which shall be established early in the weapon systems acquisition process. The purpose of this

program is to: (1) enhance the operational readiness and mission success of the defense resource; (2) identify and reduce potential vulnerabilities to security threats; (3) provide management information essential to system security planning and; (4) minimize its own impact on overall program cost and schedule [Ref. 54: p. 7]. The requirements of the SSE program is divided into four phases, the same as the acquisition phases. The detail requirements presented by the DoD are shown in Table 8 [Ref. 54: p. 8 - 14].

Most of these tasks are fulfilled by contractors with the government's contract-specific inputs, such as the classification requirement for a weapon system. To achieve a defined security level during the entire acquisition phases, the government should actively participate in the testing and validation of those tasks.

5. Industry Security Manual for Safeguarding Classified Information (DoD 5220.22-M)

The Industry Security Manual provides contractors with the provisions of the government's information security program that are necessary for safeguarding classified information entrusted to contractors who have been selected to perform on classified contracts. Issued under the authority of DoD Directive 5220.22, "DoD Industry Security Program," the manual establishes the minimum requirements for safeguarding the classified information to which contractors and their subcontractors have access or possession. The range of this classified information also covers classified foreign government information that is furnished to U.S. contractors. [Ref. 49: p. 1-1-2]

Rather than MIL-STD-1785, which provides more specific security requirements for the phases of weapon system contracts, the purpose of this manual is to provide uniform security requirements to trusted contractors. Examples include security clearances of users, security training and briefings, information classification, safeguarding classified information, and secure automated information systems operation. It reflects an effort of the DoD to demonstrate how information handling systems are securely configured or managed, and how information is securely handled by industry.

95

Table 8. Task Requirements of SSE Program

Phase I : Concept Exploration Phase		
	Goal	Identification of a broad range of security criteria and concepts which satisfy operational conditions and mission requirements.
	Task Requirements	• System Security Management Plan (SSMP) • Threat Definition and Analysis • Preliminary System Security Concept (PSSC) • Security Requirements Definition • Technology Assessments and Cost Studies • Logistic Support • Security Training Requirements • Reliability and Maintainability Program (R&M) • Preliminary Security Vulnerability Analysis • Security Classification Requirements
Phase II : Demonstration & Validation Phase		
	Goal	Translation of qualitative security criteria (developed during the concept Exploration Phase) into quantitative security criteria for specifications that can be used during the next phase.
	Task Requirements	• Adversary Mission Analysis • Updated and expanded PSSC • Review of Security Regulatory Requirements • Security Vulnerability Analysis • Security System Trade-off Analysis • System and Subsystem Specification • Manpower Impact Assessments
Phase III : Full-Scale Development Phase		
	Goal	Development of the hardware, firmware, and software components of the pre-production prototype system according to system specification, Verification of compliance with the specification requirements supported by engineering development tests, Qualification of security subsystems, and Documentation of the information required for the next phase.
	Task Requirements	• System Security Requirements Definition • Expanded SSMP • Subsystem and Interface Specifications • System Security Design • Subsystem Verification Analysis • Subsystem and System Response Analysis
Phase IV : Production & Deployment Phase		
	Goal	To ensure that defined security requirements are met in the operational system.
	Task Requirements	• Acceptance Testing • Training on Security Systems • Program Management Responsibility Transfer (PMRT) Support • Product Security

C. SECURITY CONSIDERATIONS FOR CALS

When the communications plan for implementing CALS is designed, there are very critical security considerations that should be examined prior to the actual plan. Some of these considerations are related to security policies concerning data protection, and others deal with securing methods and technologies for information. This section addresses some of the security considerations that emerged from the U.S. CALS implementation history or from other security domain technologies.

1. Security Classification

Combined with user clearances, the classification of data plays a very important role in determining the level of security protection for both single computer systems and networked systems. Actually, the security mode of operation and the requirement of adequate trusted systems discussed in the previous section are evaluated by calculating the risks of disclosing the highest classified data in the system to a user possessing the lowest clearance.

Today, the military model of hierarchical data classification is one of the most widely used data ranking methods. Unclassified, sensitive unclassified, confidential, secret, and top secret are types of data classification used in this model. The military model gives an effective basis for access control of these data. The Information Security Program Regulation presents well-defined procedures dealing with differently classified data [Ref. 50]. In terms of data integration in a data flow model (e.g., the Bel-LaPadula model), however, the strong differentiation of data types in the military model does not promise the integration of those data, since any user who has a higher level of clearance than that ascribed to the objects can access and read those objects, but cannot produce any objects with a lower level of classification [Ref. 35: p. 249]. Although higher levels of classified data are more reliable in general, the actual data processing work in this

97

model should be done with lower or, at most, the same level of classified data; thus, the trustedness of the result may be lower than expected.

On the other hand, industry uses a different data control scheme. Their intellectual proprietary data are protected by laws authorizing their patents, copyrights, or trade secrets. Yet, there are other groups of data that are highly sensitive to routine business but inadequate for those protection laws (e.g., financial data or competition sensitive data). When compared to the military classification model, most sensitive data used in industry can be categorized into a confidential data type which includes financial, proprietary, and mission-sensitive data.

When data classification requirements are determined early in the acquisition phase, CALS data classification should be done with careful consideration of data protection vs. data integration. In other words, to provide maximum data utilization in weapon systems development, only the sensitive part of documents or engineering drawings may have a higher classification for secrecy, while the other parts retain a normal classification.

The data classification rule should be specific enough to cover the inference problem, which drives sensitive data from non-sensitive data resulting from on-line query functions provided by CITIS. Although those results of query function are not predictable, the security policy concerning data classification should control inference problems by either suppressing obviously sensitive information, or by denying the query service.

2. Technical Data Rights

As mentioned earlier, CITIS will provide government access to a contractor's database, which contains government-owned data specified in the Contract Data Requirement List (CDRL), Government Furnished information (GFI), and contractor's proprietary data related to weapon system development and support. According to CITIS, for intellectual proprietary data the government shall not, as a consequence of the

delivery of a data item, acquire ownership of the data item or any rights or license to use, copy, or disclose such a data item. The extent and nature of rights that the government may acquire to use, copy, or disclose data items shall be as expressly stated in the contract [Ref. 18: p. 12].

When dealing with intellectual property, however, there is an increased risk of misuse of proprietary and business-sensitive data in digital form. No DoD regulation currently exists to assess liability of third parties for copyright or patent infringement. Even with access limitations, proprietary markings, such as proprietary legends and restrictive distribution statements, may be inadvertently deleted [Ref. 8: p. 7-37].

Thus, when the government fears disclosure of classified data handled by contractors and discontinuity of CITIS support due to the nonexistence of original contractors, the contractors fear the loss of their technical leading edge. The most prevailing belief in most government contracting activities is that the government buys too much technical data, and doesn't protect licensed data adequately [Ref. 55: p. 14]. To achieve the shared data environment, CALS requires harmonized cooperation between the government and contractors. But if the government paid more money for unlimited rights to the technical data, and still the contractors were afraid of the loss of control over their proprietary data, then the benefits of CALS from a shared common database would be hard to achieve. Therefore, to envision a fully integrated CALS environment, a strong agreement on data rights and on the following regulations should be established between the government and contractors.

3. Access Classification

The two main users of CALS data are the government and contractors of a weapon system. In reality, the contractors are composed of various groups, such as the prime contractor, teamed contractors, subcontractors, suppliers, and vendors [Ref. 18: p. 5]. As all of these groups, including the government, have their own reasons for accessing CALS data, there should be a clear policy to distribute appropriate access

rights to those groups. To preserve the ownership of data, and to protect data abuse, these access rights should be carefully analyzed and granted. At present, the CALS Implementation Guide suggests five types of access rights: view only, comment/annotate, extract/process/transform, update/maintain, and archive [Ref. 7: p. 87]. As those access rights are not mutually exclusive, a single user entry may have two or more rights.

- View Only: The ability to examine a data file without the ability to change it. This includes viewing selected portions of one or several documents, as well as side-by-side comparisons of documents.

- Comment/Anotate: The ability to evaluate and highlight for future reference or to make annotations, approvals, and comments without the ability to change the original file.

- Extract/Process/Transform: The ability to extract and modify the format, composition, and structure of all or a portion of the data into another usable form without affecting the original content or format.

- Update/Maintain: The ability to change data, either directly or through controlling software, in the active files on the host computer.

- Archive: The placing of data into a repository to preserve it for future use.

When using CITIS, the responsibility to control and maintain those access rights granted by an acquisition manager lies with the prime contractor who provides the electronically accessible database. Most of those access rights are related to the core functions of CITIS. Thus, any CITIS application provided by the contractor should support those access attributes when users access to data files or packages are stored primarily in the contractor's database. The decision to combine those access rights to each of the objects (e.g., Access Control List) or to build a separate matrix (e.g., Access Control Matrix) depends on the database construction plan. As those objects would be divided into several different classifications, there should be a well-defined mandatory access control policy to support access rights only for users who have a relevant security clearance.

100

4. Access Control using Digital Signature

When CALS is supported by a mature telecommunications infrastructure that allows on-line data transmission between the government sites and contractor sites, the users of CALS technical data must be able to exchange technical data for weapon systems. As data transmitted and processed by users will have various levels of sensitivity, there should be a trusted procedure to control access by users to only that level and category of information for which they are cleared and authorized (mandatory access control), and for which they possess a need-to-know (discretionary access control).

The mandatory access control (MAC) dictates that a user's clearance level must meet certain criteria in order for the user to access an object with either read or write privileges. The MAC policy is enforced by the underlying operating system rated above B1 TCB. The discretionary access control (DAC) allows the creator of data or programs to specify the access other users may have to information under their control. The DAC policy is enforced by a set of rules for controlling and limiting access, based on identified individuals who have been determined to have a need-to-know for the information. It provides an additional finer granularity of control within the confines of MAC.

To support these access control mechanisms, there should be a secure way to authenticate users who want to access to intellectual information. At present, enhanced access control mechanisms are provided by hardware devices (e.g., token and smart card). However, access control using those devices is restricted to a certain range of local authority; thus, it may not be used in CALS telecommunications architecture, which allows global user access across the boundary of a certain local security domain. The certified digital signature can act as a ubiquitous user identification across a local security domain. As mentioned earlier, the characteristics of digital signature, which can provide unforgeable, unalterable, nonreusable, and authentic messages are well fit for the strong authentication mechanism. The digital signature can serve for not only the access control, but also for the protection of intellectual property rights [Ref. 56: p. EI-95]. When combined with enveloping methodology (the header portion of a data package/element)

already provided by MIL-STD-1840B, the digital signature can prevent unauthorized copying and use via digitally signed and certified property labels.

However, prior to use of digital signature, a nationwide or even worldwide policy should be established for handling digital signature certificates that validate the identity of a user.

5. International Data Exchange

From nation to nation, international data exchange is complicated by differences in the treatment of intellectual data. Some nations do not recognize or protect intellectual property. Export licensing of technical data also creates a barrier to international cooperation using on-line data transfer, such as CITIS [Ref. 8: p. 7-38].

At present, the Korean defense industry has the research and development capacity for advanced weapon systems, but they still largely depend on foreign technology for core technological components [Ref. 57: p.143]. As core technology contains highly sensitive or classified information, there should be a set of restriction policies to support on-line transmission of the information. DoD 5200.1-R, Information Security Program Regulation, presents such restrictions for information resulting from Foreign Military Sales (FMS) or Direct Commercial Sales, based on the assumption that this information would be shipped via off-line media [Ref. 50: p.VIII-4], yet it doesn't specify any method allowing on-line interaction between the U.S. and foreign countries.

As CALS is used to establish the paperless environment in the future, there should be a way to enable international cooperation in developing advanced weapon systems. Although encryption may help international data exchange, there should be a mutual agreement on the procedure and actual cryptosystems to convince each other that the information will be protected in a same or an equivalent manner in each country prior to the data interchange using encryption.

6. Weapon System Phase and IWSDB

The construction of the IWSDB is the essential part of CALS implementation. IWSDB is a logical database that provides multi-weapon systems technical information, regardless of the physical location of actual data storage. It should contain all digital data required to support the life-cycle of a weapon system. As mentioned earlier, extensive network capabilities and flexible open system architecture are two basic requirements to accomplish this integrated database.

The IWSDB should include military data depositories and contractor's databases. On-line data transmission among those databases will be supported by CITIS applications. To enable CITIS between users and information providers, however, interface parameters should be established (e.g., data elements, Global Data Dictionary and Directory (GDD/D), interface protocol). On the basis of security consideration, to control physically distributed databases is not an easy task. By its distributed characteristics, those databases may allow different classifications to the same level of data. As the strength of security is only as good as its weakest point, any weak access point to the databases may downgrade overall CALS security. Thus, the security policy governing database security should be able to control distributed, multi-level weapon systems databases.

When on-line data transmission is enabled through CITIS, the main responsibility of information security lies with the contractors. The contractors should fulfill basic security requirements, such as risk analysis, regular backup, and access monitoring. However, it is not realistic to assign security responsibility to contractors for the entire life-cycle of a weapon system. Since most data transmission is anticipated to occur at the later phase of the life-cycle, during many users request technical information to maintain their weapon systems (e.g., technical manuals), the contractors should be able to control users' access requests on their databases. It is more realistic to construct regional CALS data repositories to support the later phase of weapon systems. They can be constructed in selected military CALS sites. As those data repositories are within the domain of

military information security, they will reduce certain amount of security risks. Also, they may act as backup systems for weapon systems information. The main advantage of constructing regional data repositories is the reduced requirement of on-line data transmission when regional sites are carefully selected by a actual data traffic analysis. To support this plan, the acquisition manager should carefully consider the future requirement of CALS data.

7. Multi-Level Security and Security Risks

CALS requires a secure architecture to control the effective utilization of technical information related to weapon systems life-cycle among military CALS sites and contractors. Most of the technical information used to support weapon systems is unclassified but sensitive data, but there also could be classified data. Thus, to provide adequate protection for both unclassified and classified data, and for other resources, CALS sites should be equipped with trusted systems, including computing systems and other networking components, which can handle differently classified data with DAC and MAC. Table 7 suggests that the components of CALS networks should be rated at least the B1 level of trusted computing systems to support MAC and DAC. Also, since not all users have a clearance or formal access approval for all technical data provided by IWSDB, the operating mode shall be a multi-level security mode.

To meet the security requirement of the entire CALS communications infrastructure, there should be a way to accredit the networked systems at the B1 level, which are operated in multi-level security mode. On the basis of the interconnection rule, which is provided by TNI Part I, each device in the network must be separately accredited to operate in an approved security mode of operation, and with a specific accreditation range. However, even when the interconnection rule is followed, there may be other potential security problems that will require the implementation of additional constraints on the network, a global view of the network which is provided by TNI Part II. This global view of the network addresses two potential damages: propagation of

local risk and the cascading problem. The propagation of local risk is caused by weaknesses in other systems connected to the network, and the cascading problem exists when an attacker can take advantage of network connections to reduce the nominal system resistance against leaking information across a range of sensitivity levels [Ref. 52: p. 39 - 48].

The first problem can be prevented by logically or physically disconnecting the untrusted systems. For the CALS telecommunications network, those systems that are not related to provide or use technical data should be disconnected from the network, or else all other trusted systems should be equipped with cryptographic devices to logically isolate those untrusted communications. The cascading problem is usually caused by the installation of malicious software on the lowest resistance point in the network. To prevent this problem, there should be a security policy governing configuration management to prohibit installation of unscrutinized software, or use end-to-end encryption between trusted hosts.

CALS technical data transmission supporting weapon systems development and maintenance may allow a common untrusted path between military CALS sites and contractors for the cost-effective means of a common data carrier. Also, other connections within military CALS sites and contractors may be allowed, even after CALS is implemented. Thus, the environment of CALS telecommunications suggests that the use of an encryption tool is a more favorable method than the disconnection or isolation of other networks that are not related to CALS telecommunications.

D. PROPOSED SECURE TELECOMMUNICATIONS ARCHITECTURE

This section summarizes the analysis presented in the previous chapters to provide a secure telecommunications architecture. The main purpose of this section is to envision the openness of connecting various systems for data integrity, and to suggest security requirements for data protection. In general, any protection mechanism will cause a certain amount of overhead from integration. However, without adequate

protection, the integration will be easily ruined, and the true meaning of integration will not be accomplished. Thus, it is important to treat security requirements as part of the essential building blocks of the CALS telecommunications plan.

1. Open System Architecture and Internetworking

a. Open System Employment

To make networks interoperable, there are two important points that should be considered prior to the actual plan: the network protocols and applications. The two major protocol suites that promise open system networking are OSI protocols and TCP/IP protocols. Considering the networking trends in the Korean government and industry, TCP/IP protocols are more widely accepted as providing the best interoperability to their heterogeneous computers. Continuous growth of the Internet gives a momentum toward further enhancement of TCP/IP protocols and other network applications using TCP/IP. For the CALS data communications, either TCP/IP applications, such as FTP, or the contractor-developed applications using TCP/IP protocols will be used. On the other hand, as OSI protocols are also gaining popularity with their X.400 message handling service and X.500 descriptive naming services (which are very important for secure message delivery and public key certificates), these two standards should be considered as parts of essential applications along with other TCP/IP applications. The application gateways bridging TCP/IP protocols and OSI protocols are already available in the present market place; thus, those gateways don't need additional development efforts. However, the two OSI applications still are not fully developed for actual usage, and there also are efforts to develop equivalent applications using TCP/IP protocols, so it will be more flexible to decide the gateway option in the mid-term phase of the CALS telecommunications plan.

b. *Local Area Connectivity*

When LAN, used in the CALS telecommunications, is defined as a network connecting computing devices within a military CALS site or a contractor site, the connectivity of those devices can be achieved by various means of networking technologies. Actually, any LAN technology can be used with TCP/IP protocols without affecting the long-haul connectivity. At present, FDDI is one of the best choices for LAN, providing high-bandwidth capacity to the network applications. Not only for LAN, FDDI can also be used for a Metropolitan Area Network (MAN) with its ability to connect across tens of kilometers [Ref. 58: p. 64]. Thus, if there were a specific location where both military CALS site and contractors (including subcontractors) were dispersed within a city, FDDI can act as both LAN and WAN, with more than 100 Mbps bandwidth.

At present, even if already-employed LAN technologies are not FDDI, the capacity in these technologies is larger than the current WAN capacity. Therefore, the CALS cites that use other LAN technologies can continuously use their LAN connection, at least until the WAN capacity overcomes the capacity of their LAN. However, newly employed LAN should consider FDDI as the most adequate technology.

There should be a consideration of wireless LAN technologies for the specific CALS sites that require mobile computing capability (e.g., naval shipyards). Electronic TMs are examples that require mobile computing for weapon systems maintenance. Currently available wireless LAN technologies are: infrared lightwave, spread spectrum, and microwave radio. Although wireless LAN technologies will be necessary for these maintenance purposes, the decision to select a specific LAN technology will be based on the characteristics of the specific CALS site.

c. Wide Area Connectivity

For CALS data transmission, there should be a long-haul connectivity between military CALS sites and contractors. This can be provided by either newly employed, dedicated lines between them, or by common carriers used for other communication purposes. To construct a WAN for only CALS purpose is not a cost-effective method. Thus, for CALS communication, already installed, or planned future common carriers are more favorable.

For communications between CALS sites, the DDN (KDDN) can be used. The KDDN was planned in 1992, and the first stage of KDDN will be completed by the end of 1995. At present, based on the X.25 frame relay, the backbone capacity of KDDN varies between 9.6 Kbps and 1.544 Mbps, whereas local branched lines only support 9.6 Kbps. This may be enough for a small amount of data transmission, but, the same as for U.S. DDN, it cannot be a cost-effective media to handle on-line transmission of extremely large technical data transmission. However, as it is anticipated that the KDDN will have large bandwidth in its future stages, along with the overall development plan of the Korean Information Infrastructure (KII), CALS communications between the military sites should take into account the development phases of the KDDN.

For communications between military sites and contractors, the present commercial Internet (e.g., KORNET) can be used with a bandwidth of T1 (1.544 Mbps). The T1 capacity may give a reasonable bandwidth for CALS data transmission, although the required bandwidth may vary, depending on the amount of communications between those sites. As the capacity of the commercial Internet will be increased along with the KII development plan, the future capacity of the commercial Internet will give sufficient bandwidth for CALS data transmission between military sites and contractors.

At present, the Korean government places a high priority on the construction of a robust, information-sensitive, socio-economic infrastructure, the Korea Information Infrastructure (KII). The KII is divided into two categories: the New Korea Net-Government (NKN-G) for the government sector, and the New Korea Net-Public

(NKN-P) for public sector. [Ref. 59] The KII will employ ATM for their WAN technology. Both the NKN-G and NKN-P have a three-phased plan to construct a high-bandwidth backbone, and to implement related services. The planned networking capacity of the KII is shown in Table 9. As the KDDN will be part of the NKN-G (even though it is separately constructed for security purposes) while the commercial Internet is being integrated into the NKN-P, the telecommunications plan for CALS should follow the phased plan of the KII to achieve a cost-effective means of on-line data transmission.

Table 9. Network Capacity of the KII

Stages	NKN-G	NKN-P

Groundwork stage (1995-1997)	• Backbone capacity
	   - between major cities: 622-2.5 Gbps
	   - between major cities and hub cities: 622 Mbps
	• Interconnection between LAN: above 45 Mbps
		• Backbone capacity:
		   155-622 Mbps
		• Local subscriber loop:
		   2 Mbps class

Diffusion stage (1998-2002)	• Backbone capacity
	   - between major cities: above 2.5 Gbps
	   - between major cities and hub cities: 622-2.5 Gbps
	• Interconnection between LAN: above 155 Mbps
		• Backbone capacity:
		   2.5-10 Gbps
		• Local subscriber loop:
		   45-155 Mbps

Completion stage (2003-2015)	• Backbone capacity - several tens of Gbps up to several Tbps	• Backbone capacity: 100 Gbps • Local subscriber loop: 155 Mbps

2. Security Plan for CALS Telecommunications

Currently, the Korean military has security regulations for secure computing and communications. However, to control information systems security in a highly integrated environment, there should be more specific security domain standards and regulations. For the successful CALS implementation, there is an urgent necessity to set an overall security policy governing the security concerns about technical information used in the CALS environment. The domains of those security requirements are various. The overall security policy should cover computer security, information security, and communications security, as well as physical security of CALS sites. As part of this

overall security policy, the security plan for CALS communications should include: secure computer systems acquisition and management, data and user classification, data protection mechanisms, rules for information transfer, and roles of security administrators.

a. Systems Acquisition and Management

For computer systems acquisition and management, there should be functional criteria for secure computing systems (including communicational devices) that will be used in the CALS environment. Most of the workstations used in Korea were imported from other countries without security considerations. For those systems, the policy must define add-on security devices and software. Also, the policy will help future acquisition decisions about computing systems and related networking devices. The policy should provide CALS sites with the procedural guidance required to maintain the operability of systems (e.g., risk analysis, regular backup, monitoring, and contingency plan), which is tailorable to match the specific working environment of the site.

b. Data and User Classification

The security policy should provide the criteria to classify technical information used in a weapon systems life-cycle. For technical data, the classifying criteria should reflect the integrity of information (i.e., minimum restrictions on technical data) to fully utilize technical information within a distributed environment. It will also define the security head portion of any digitized data element to visualize the security label of information. The security policy must provide the criteria required to set the clearance of non-governmental users, and related procedures to assign the clearance (e.g., security training and briefing). For the integrated CALS environment, the relationship between users and technical data will be governed by access attributes (e.g., access privileges, and

release authority for information transfer). Those attributes will be assigned to each data elements through database control mechanisms (e.g., ACL, ACM).

c. Data Protection Mechanism

The policy must define the actual methods to protect information from unauthorized use, wire tapping, and other security attacks. Most communication security can be provided by encryption. Link-encryption (which can be performed without the knowledge or participation of a user's process) can be primarily used, since the users of CALS data may not have the background to implement an appropriate encryption method. Later, end-to-end encryption, which requires the user's responsibility for performing encryption, should be employed to give the user a choice of when to use encryption and which encryption algorithm to use. In a highly integrated environment, it will be more proper to protect CALS data by differentiating the encryption mechanisms with the types of classifications.

There should be two categories to specify the security mechanisms: mandatory and tailorable. Mandatory mechanisms should define the types of cryptographic devices and applications, secure key management, and required reports and documentation. Tailorable mechanisms should represent the site's unique situation, and provide the mechanisms for access control, auditing, database management, communication channel analysis, a security recovery plan, and other tailorable functions required to maintain information security at a site.

d. Rules for Information Transfer

The security policy should define the rules by which technical information is securely transferred from one site to another. It should be embedded within guidance standards such as MIL-STD-1840B and CITIS, or separately defined in an information handling guidance. The rules will define the procedures required to handle an element of

111

information, or a package of information within differently configured sites. To protect certain levels of classified information, the rules should define the way in which information is upgraded or downgraded to support the overall access control mechanism. Those rules will also specify procedures to classify results of on-line queries to prevent the inference problems that usually happen in a database security.

e. Role of Security Administrator

The security policy should define specific roles of security administrators who take the most responsibility related to site security. These roles should consist of regular duties and special requirements reflecting specific roles and the environment of a site. In an environment dealing with paper-based, classified information, there might be little cooperation between acquisition managers and security administrators. However, in a highly integrated environment, where information is transferred at light speed, there should be high-degree of cooperation between these two personnel, to provide information security without affecting weapon systems development and maintenance. Thus, the security administrators should be aware of overall acquisition procedures and data flows within a weapon system life-cycle, in addition to information security requirements.

3. Secure CALS Telecommunications Architecture

To establish an interoperable CALS environment, the CALS telecommunications implementation will reflect the time frames of national information infrastructure development plan. Also, the close relationship between telecommunications and network security suggests that the network security development plan will have the same time frames. The phases can be divided into three terms: the near-term, mid-term, and long-term phase.

In the near-term phase, the current KDDN will be used to connect military CALS sites, while the commercial Internet will provide a communication channel between military sites and contractors. In the mid-term phase, the second phase of KDDN will provide a high band-width communications channel between military CALS sites, while the diffusion stage of NKN-P will provide the communications channel for military CALS sites and contractors. In the long-term phase, it is anticipated that CALS will have enough band-width for on-line data transmission; thus the telecommunications implementation plan will focus on the extension of the on-line CALS services.

For telecommunications security, the near-term phase will focus on the establishment of security policy, and on the development of enhanced cryptographic devices. In the mid-term phase, connection-oriented security will be implemented via domestic commercial equipment. In the long-term phase, management of telecommunications security will be focused as a network security model to influence the overall military information infrastructure.

a. Near-Term Phase

For CALS telecommunications, current KDDN can be used as a connection channel between military CALS sites. However, as the capacity of current KDDN is not enough for transmitting technical information, only limited data traffic will be allowed. For the communication between contractors and military CALS sites, the commercial Internet will provide a communications channel, either as a direct connection or as a common carrier (e.g., VAN), depending on the availability of the service. The communications security will be provided by a link encryption device, which is currently used for KDDN security, and by an isolation policy, which denies any connection except the CALS-specific access requirements.

In this phase, the effort to implement CALS telecommunications will be focused on four areas: (1) the digitization of technical data and bulk data delivery through the adaptation of MIL-STD-1840B, (2) data traffic analysis between data repository and

113

actual users, (3) construction of high band-width LANs, and (4) preparation of TCP/IP protocols-equipped computers and network devices.

For communications security, there are many more requirements that should be done during the near-term phase. Those requirements are: (1) establishment of security policy and related regulations concerning computer security, information security, and telecommunications security, (2) provision of CALS-specific security policy governing the role of information security in weapon systems acquisition phases, in which information is shared with non-military organizations, (3) development of add-on security devices and applications providing additional security features to non-secure computing systems, (4) construction of security gateways to deny any connection requirements from unauthorized users, (5) configuration for a closed community within military CALS sites and contractors, (6) analysis of the strength of cryptographic algorithms that were not developed in Korea, and their availability in the international environment, and (7) developing enhanced cryptographic algorithms and security devices that minimize the security overhead against telecommunications performance.

b. Mid-Term Phase

In this phase, as a part of the second stage of the NKN-G project, the DISN is expected to support all required CALS telecommunications requirements within military CALS sites. In a public communications domain, the NKN-P project will also support the connection between military CALS sites and contractors. As on-line CALS data transmission will be realized in this phase, a secure CALS telecommunications implementation should focus on the on-line functionality of telecommunications and connection-oriented security service.

For CALS telecommunications, the requirements are: (1) maintaining wide-area connectivity utilizing ATM technology, (2) development of CITIS applications, which will enable on-line data transfers from the contractor's data depository to military CALS users, (3) continuous development of networking applications using advanced

114

information technologies, and (4) simplifying the management of interfaces between the local and wide-area environment to maximize the integrity of information.

On the other hand, the telecommunications security should provide adequate protection for the real-time data transmissions. To support on-line CALS telecommunications, connection-oriented security mechanisms should include: (1) developing public key encryption technology and key management technology, (2) simplifying security procedures required in the multi-level, integrated information environment through developing a portable device for access control, user authentication, and key exchange, (3) development of intelligent gateways to control real-time user queries while maintaining original data classifications criteria (i.e., protection against inference attacks), (4) interaction with other security service mechanisms to achieve overall CALS security, and (5) provision for international data exchange to accelerate weapon systems development.

c. Long-Term Phase

The KII is expected to be completed in this phase. Through the nation-wide information infrastructure, CALS data can be easily transmitted and the use of CALS data can be optimized. In this phase, CALS telecommunications will focus the expansion of the interactive services directly connecting any technical information to its actual user through automated security procedures. However, highly integrated information systems are more vulnerable to security attacks than isolated systems. It may be very difficult to evolve from a paper-based information environment to a integrated, digitized information environment. But, it will be much more difficult to return to the old stage from an integrated environment. Since the dependency on automated information systems has been increasing, it may provide an easily identifiable target for any malicious attempt. This is one of the reasons why currently U.S. makes provisions for "Information Warfare." Thus, the goal of secure CALS telecommunications implementation in the

long-term phase should focus on the maintainability of the CALS telecommunications architecture.

To support such a goal in this phase, the effort to implement CALS telecommunications should focus on: (1) continuous development/adaptation of telecommunications technologies, (2) migration from a closed community to an open community to optimize the information infrastructure, and (3) ensuring minimum redundancy on its information architecture.

The telecommunications security in this phase deals with requirements such as: (1) development of secure telecommunications protocols, such as networking protocols and protection mechanisms using encryption, (2) Refinement of security management on CALS telecommunications with distributed networks management functions, and (3) provision of a multilevel secure network model to influence overall military information infrastructure. Table 10 summarizes the requirements suggested for the secure CALS telecommunications architecture.

Table 10. Phased Approach for Secure CALS Telecommunications Architecture

Phase	Telecommunications Requirements	Security Requirements
Near-term	• Digitize technical data • Analyze data traffic requirements • Construct high band-width LANs • Use TCP/IP protocols for interoperability	• Set security policy and related regulations • Provide CALS-specific security policy • Develop security devices and applications • Construct security gateways • Configure closed community • Analyze strength of cryptographic algorithms • Develop enhanced cryptosystems
Mid-term	• Utilize ATM technology for WAN • Develop CITIS applications • Develop networking applications • Simplify interface management	• Facilitate public key technology • Simplify security procedures • Develop intelligent gateways for databases • Interact with other security services
Long-term	• Develop/adapt new technology • Evolve to an open community • Ensure minimum redundancy	• Develop secure telecommunications protocols • Refine security management on CALS telecommunications • Provide a multi-level secure network model

VI. CONCLUSION

CALS is more than a collection of automated information systems. It is a strategy to increase the national potential which can employ rapidly evolving information technology. The benefits that could be achieved from CALS include not only efficient or cost-effective information management and control in a national defense environment, but also an advanced national competitive power in the highly competitive, information technology-based international market place. In the U.S., the term CALS is not limited to the defense industry. It is extended to a new concept, such as the Enterprise Integration Strategy, which can change all conventional data processing works to an equivalent or even an enhanced, digitized version.

Although those benefits may not be achieved in a short period, the Korean government and defense industry should invest in CALS for the future. The MND must initiate a pilot project to modernize toward a cost-effective CALS solution for acquiring and managing digitized information by means of joint service systems. Also, the industry must enhance their information infrastructure, and increase their international competitiveness.

To achieve streamlined interoperability, the efforts to implement CALS in Korea should start with the adaptation of CALS standards, a common bridge that enabling organizations to exchange and share information more efficiently. Streamlined information processing will provide the opportunity to do business in the most efficient way by removing any redundant and unnecessary steps. Emerging CALS standards and information technologies to enable streamlined business processes should be adapted early or developed by the Korean industry.

To support this working environment, the telecommunications capability acts as one of the most significant part of CALS infrastructure. Without connectivity, any effort toward a highly integrated working environment cannot accomplish its goal. The most widely used telecommunications protocols should be selected, and continuously evolved

119

to enable a better opportunity to integrate a separated working environment. A telecommunications capacity should be achieved via the national effort to develop a nation-wide information infrastructure. The CALS initiative will demonstrate how the nation-wide infrastructure can be used to enhance cooperation between the government and industry, and contribute a large portion of return on the initial investment.

At present, however, to provide appropriate means of protection for the confidentiality of CALS information is one of the key challenges. In a highly integrated working environment, the potential vulnerability dramatically increases while the importance of each data element is increasing. Any damage to the data used in the integrated working environment will cause much more cost for recovery than one in a isolated working environment. Even worse, the potential damage to CALS technical data may compromise national security. As any method to protect this information usually causes a certain amount of security overhead to the integrated CALS environment, the decision to select security mechanisms should be made based on the comparison between security and integrity, in terms of efficiency, effectiveness, and availability.

"Perfect security" may not be possible. Rather, security mechanisms will reduce the degree of information systems vulnerability to an acceptable level. Among the various security mechanisms, the most effective protection method against network attacks is encryption. Currently developed public key algorithms provide a much more flexible way to ensure data authenticity and confidentiality. Along with a well-defined security policy and related regulations, public key algorithms can provide most of the security service needed for sensitive information. The development of publicly available cryptography will also contribute to the security of a national information infrastructure.

In the CALS environment, the acquisition manager, other government users of technical data, and the contractors have a shared responsibility to provide an adequate level of protection in all CALS-related delivery and access modes. As the security is only as good as its weakest point, all of the security contributors should cooperate to accomplish overall CALS information security.

LIST OF REFERENCES

1. CALS Industry Steering Group, "CALS Vision," CALS EXPO '94, Proceedings and Reference, December 94.

2. Doby, Joan S., "Computer-aided Acquisition and Logistic Support Telecommunications Security Plan," Logistics Management Institute, January 1991.

3. DoD, "CALS Strategic Plan," October 1993.

4. Morgan, Roy S., Editor, "A Collection of Technical Studies Completed for the Computer-aided Acquisition and Logistic Support (CALS) Program Fiscal Year 1988," U.S. Department of Commerce, April 1990.

5. Smith, Joan M., "An Introduction to CALS: The Strategy and the Standards," May 1990.

6. CALS Industry Steering Group, "CALS Reality, An Introduction to CALS," CALS EXPO '94, Proceedings and Reference, December 1994.

7. DoD, "MIL-HDBK-59B, Continuous Acquisition and Life-Cycle Support (CALS) Implementation Guide," June 1994.

8. Navy CALS Resource and Implementation Cooperative (RIC), "Navy/Marine Corps Manager's Desktop Guide for CALS Implementation," Naval Air Warfare Center, Aircraft Division, Indianapolis, September 1994.

9. Paltzman, Alan, "Memo from DISA Allowing CALS Standards and Specifications to be used Without Waivers," Navy CALS in Action, http://navysgml.dt.navy.mil/waiver.html, March 1995.

10. Knox, Rita E., Ph.D., Kumar, Sanjiv, and Gelenius, Sherry, "Choosing the Right Standard for Data Representation," CALS Journal, Fall 1992.

11. CALS Industry Steering Group, "Standards for CALS," CALS EXPO '94, Tutorial Program, December 1994.

12. Fuhs, Hans Georg, "Application of the Continuous Acquisition and Life-Cycle Support (CALS) Initiatives to the Evolved Seasparrow Missile Program," Master's Thesis, Naval Postgraduate School, March 1995.

13. DoD, "MIL-HDBK-59A, Computer-aided Acquisition and Logistic Support (CALS) Program Implementation Guide," September 1990.

14. Smith, Delores, "EDI with Technical Data - A Full Scale Test," CALS Journal, Summer 1992.

15. Beazley, William G., Editor, "Federal Government Increases Commitment to Electronic Commerce," CALS/CE Report, Vol. 7, No. 12, December 1994.

16. Bloom, Howard M., "STEP - Standard for the Exchange of Product Model Data," CALS Journal, Summer 1992.

17. Doby, John S., "Computer-aided Acquisition and Logistic Support Telecommunications Plan," Report PL810R1, Logistics Management Institute, Bethesda, Maryland, August 1989.

18. DoD, "MIL-STD-974, Contractor Integrated Technical Information Service (CITIS)," August 1993.

19. U.S. Air Force, "Air Force CALS Test Network Handbook," September 1994.

20. DeLaura, Frances L., Sharp, Steven J., Clark, Richard, "Assessment of DoD and Industry Networks for CALS Telecommunications," Logistics Management Institute, Bethesda, Maryland, December 1987.

21. Stallings, William, "Data and Computer Communications, Fourth Edition," Macmillan Publishing Co., 1994.

22. DoC, "FIPS PUB 146-1, Government Open System Interconnection Profile (GOSIP)," April 1991.

23. Olsen, Florence, "TCP/IP Wins Big in the Federal Market as Novell IPS Declines," Government Computer News, September 5, 1994.

24. Quarterman, John S., "The Demise of GOSIP," http://netlab.itd.nrl.navy.mil/GOSIP/Demise_of_GOSIP, October 1994.

25. House, Walter R., "NIST Went Too Far in Tossing Out the GOSIP Mandate," Government Computer News, October 17, 1994.

26. Feibel, Werner, "Novell's Complete Encyclopedia of Networking," Novell Press, 1995.

27. Comer, Douglas E., "Internetworking with TCP/IP, Volume I, Principles, Protocols, and Architecture," Prentice Hall, 1991.

28. Clark, Russell J., Ammar, Mostafa H., and Calvert, Kenneth L., "Multiprotocol Interoperability In IPng," Internet Draft, Georgia Institute of Technology, January 1994.

29. Nassif, Tobias A., "Supporting the Fleet: Taking Workflow to the Waterfront," Master's Thesis, Naval Postgraduate School, Monterey, CA., March 1995.

30. Brewin, Bob, "DoD Releases Strategy for Global Network," Federal Computer Week, Vol. 9, Num. 5, March 1995.

31. Krol, Ed, "The Whole Internet, User's Guide & Catalog, Second Edition," O'Reilly & Associates, Inc., 1994.

32. Houser, Walter R., "The Internet is Getting Updated for the 21st Century," Government Computer News, August 29, 1994.

33. CNO, "Guidelines for Naval Use of the Internet," R 212001Z-JUL-95, July, 1995.

34. Endoso, Joyce, "$5 Billion Later, CALS Initiative is 'in Disarray,' Glenn, GAO say," Government Computer News, October 17, 1994.

35. Pfleeger, Charles P., "Security In Computing," Prentice Hall, 1989.

36. Stallings, William, "Network And Internetwork Security, Principles And Practice," Prentice Hall, 1995.

37. Fhan, P., "Answers to Frequently Asked Questions About Today's Cryptography," RSA Laboratories Report, September 1993.

38. Kaufman, Charlie, Perlman, Radia, and Speciner, Mike, "Network Security, Private Communication in a Public World," Prentice Hall, 1995.

39. Terisa Systems, "Frequently Asked Questions about Terisa Systems, Transaction Security and the Secure Web Toolkits," http://www.terisa.com/faq.html#tech.

40. Minahan, Tim, "DSS Users Get Boost from NIST," Government Computer News, June 27, 1994.

41. RSA Laboratories, "RSA's Frequently Asked Questions about Today's Cryptography, Miscellaneous," RSA Data Security Inc., http://www.rsa.com/rsalabs/faq/faq_misc.html, May 9, 1995.

42. Rescorla, E. and Schiffman, A., "The Secure HyperText Transfer Protocol," Internet-Draft, Enterprise Integration Technologies Inc., December 1994.

43. Hickman, Kipp E.B., Elgamal, Taher, "The SSL Protocol," Internet Draft, Netscape Communications Corp. http://www.mcom.com/newsref/std/SSL.html, June 1995.

44. Wack, John P. and Carnahan, Lisa J., "Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls," National Institute of Standards and Technology, November 1994.

45. Cheswick, William R. and Bellovin, Steven M., "Firewalls and Internet Security, Repelling the Wily Hacker," Addison-Wesley Publishing Company, November 1994.

46. Schivley, Jody L., "Network Security and The NPS Internet Firewall," Master's Thesis, Naval Postgraduate School, Monterey, CA., September 1994.

47. DoD, "MIL-STD-1840B, Automated Interchange of Technical Information," November 1992.

48. DoD, "DoD 5200.28-STD, Department of Defense Trusted Computer System Evaluation Criteria," December 1985.

49. DoD, "DoD 5220.22-M, Industrial Security Manual for Safeguarding Classified Information," January 1991.

50. DoD, "DoD 5200.1-R, Information Security Program Regulation," June 1988.

51. National Computer Security Center, "NCSC-TG-027, A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems," May 1992.

52. National Computer Security Center, "NCSC-TG-011, Trusted Network Interpretation Environments Guideline," August 1990.

53. National Computer Security Center, "NCSC-TG-005, Trusted Network Interpretation," July 1987.

54. DoD, "MIL-STD-1785, System Security Engineering Program Management Requirements," September 1989.
55. Carter, Robert K., "Technical Data Rights in a CALS Environment," Master's Thesis, Naval Postgraduate School, Monterey, CA., December 1994.

56. Craft, P. James, Cartier, N. Gene, and Hampel, E. Viktor, "New Federal Standards Provide Integrity and Confidentiality for CALS and EDI," CALS EXPO '94, Proceedings and Reference, December 1994.

57. Kim, Chul Whan, and Kim, Wha Soo, "Direction for the CALS Implementation Policy for Korea," Korean National Defense University, December 1993.

58. Malamud, Carl, "Stacks, Interoperability in Today's Computer Networks," Prentice Hall, 1992.

59. Korean Ministry of Information and Communication, "The Korea Information Infrastructure: Blueprint for Implementation," http://newnet.kii.go.kr:80/s-plan/e-plan/blue-html, 1995.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   Cameron Station
   Alexandria, VA 22304-6145

2. Library Code 052 2
   Naval Postgraduate School
   Monterey, CA 93943-5000

3. Professor Myung W. Suh 1
   Department of Systems Management (Code SM/Su)
   Naval Postgraduate School
   Monterey, CA 93943-5000

4. Professor Rex Buddenberg 1
   Department of Systems Management (Code SM/Bu)
   Naval Postgraduate School
   Monterey, CA 93943-5000

5. Capt. Bae, Kichan 2
   Seoul City, Nowon Ku
   Sanggye Dong, Ju Gong Apt. 1413-105
   Rep. of Korea, 139-209

6. Woodang Library 1
   Seoul City, Nowon Ku
   Kong Neung Dong, P.O. Box 77
   Korea Military Academy
   Rep. of Korea, 139-799